November 2025

National Risk Assessment-Follow-up Report

NATIONAL PUBLIC SAFETY COMMISSION

Legal Abbreviations

Abbreviations for laws are as follows:

[Abbreviation]	[Law]
FEFTA	Foreign Exchange and Foreign Trade Act (Act No. 228 of 1949)
Mobile Phone Improper Use Prevention Act	Act on Identification, etc., by Mobile Voice Communications Carriers of their Subscribers, etc., and for Prevention of Improper Use of Mobile Voice Communications Services (Act No. 31 of 2005)
International Terrorist, etc. Asset-Freezing Act	Act on Special Measures Concerning Asset Freezing, etc. Conducted by Japan Taking into Consideration United Nations Security Council Resolution 1267, etc. (Act No. 124 of 2014)
Payment Services Act	Payment Services Act (Act No. 59 of 2009)
Investment Act	Act Regulating the Receipt of Contributions, Receipt of Deposits and Interest Rates (Act No. 195 of 1954)
Act on Punishment of Organized Crimes	Act on Punishment of Organized Crimes and Control of Crime Proceeds (Act No. 136 of 1999)
Act on Punishment of Terrorist Financing	Act on Punishment of Financing to Offences of Public Intimidation (Act No. 67 of 2002)
Immigration Control Act	Immigration Control and Refugee Recognition Act (Cabinet Order No. 319 of 1951)
	Act on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007)
Enforcement Order of the Act on Prevention of Transfer of Criminal Proceeds	Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds (Cabinet Order No. 20 of 2008)
Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds (Ordinance of the Cabinet Office, Ministry of Internal Affairs and Communications, Ministry of Justice, Ministry of Finance, Ministry of Health, Labour and Welfare, Ministry of Agriculture, Forestry and Fisheries, Ministry of Economy, Trade and Industry, and Ministry of Land, Infrastructure, Transport and Tourism No. 1 of 2008)
Amusement Business Act	Act on Control and Improvement of Amusement Business, etc. (Act No. 122 of 1948)
Anti-Boryokudan Act	Act on Prevention of Unjust Acts by Organized Crime Group Members (Act No. 77 of 1991)
Anti-Drug Special Provisions Act	Act on Special Measures for the Narcotics and Psychotropics Control Act, etc., and Other Matters for the Prevention of Activities Encouraging Illicit Conduct and Other Activities Involving Controlled Substances through International Cooperation (Act No. 94 of 1991)

Table of Contents

Introduction ······ *- 1 -*

[Overview of the NRA-FUR 2025] ······ *- 2 -*

Section 1. Risk Assessment Method ······ ***- 6 -***

1. History ······ **- 6 -**

2. Purpose ······ **- 7 -**

3. Assessment Method ······ **- 7 -**

(1) Assessment Method ······ - 7 -

(2) Information Used in the Assessment ······ - 9 -

4. Updates to the NRA-FUR ······ **- 10 -**

(1) Major Updates to the NRA-FUR up to Last Year ······ - 10 -

(2) Major Changes in NRA-FUR in Light of Recent Changes in Situations ······ - 11 -

Section 2. Environment Surrounding Japan ······ ***- 12 -***

1. Geographic environment ······ **- 12 -**

2. Social environment ······ **- 12 -**

3. Economic environment ······ **- 12 -**

4. Criminal environment ······ **- 13 -**

(1) Domestic Crime Situation ······ - 13 -

(i) Number of Recognized Criminal Offence Cases

(ii) Fraud (Online and Telephone Fraud and Investment/Romance Fraud Via Social Media)

(iii) Organized Theft and Trafficking of Stolen Goods

(iv) Illicit Commercial Practices Offences (Investment Fraud and Commercial Transaction Scam)

(v) Cyber Crimes

(vi) Gold smuggling

(vii) Online Casinos

[Topic] The Actual Situation and Characteristics of Online Casinos ······ *- 24 -*

[Comprehensive Measures to Protect People from Frauds 2.0] ······ *- 27 -*

(2) Terrorism Situation ······ - 29 -

Section 3. Analysis of Money Laundering Cases ······ ***- 30 -***

1. Offenders ······ **- 31 -**

(1) Anonymous and fluid criminal groups ······ - 31 -

(i) Characteristics

(ii) Revenue-Generating Crimes

(iii) Modus Operandi of ML Offences Involving Anonymous and Fluid Criminal Groups

(2) Boryokudan ········ - 39 -

(i) Characteristics

(ii) Typologies

(3) Crime Groups of Foreigners in Japan ········ - 41 -

(i) Characteristics

(ii) Typologies

2. Predicate Offences ········ - 45 -

(1) Major Predicate Offences ········ - 45 -

(i) Fraud

(ii) Computer fraud

(iii) Theft

(iv) Violation of the Investment Act/Money Lending Business Act

(v) Habitual Gambling/Running a Gambling Venue for Profit

(vi)Violation of the Immigration Control and Refugee Recognition Act

(vii) Violation of the Amusement Business Act/Violation of the Anti-Prostitution Act

(viii) Trafficking in person offences

(ix) Investment Fraud (Violation of the Financial Instruments and Exchange Act.etc)

(x) Drug-related Offences

(2) Predicate Offences of International Concern ········ - 53 -

(i) Bribery and corruption

(ii) Tax Evasion

(iii) Environmental Offences

3. Major Transactions Misused for Money Laundering ········ - 56 -

(1) Major Transactions Misused for Money Laundering ········ - 56 -

(2) Measures to combat crimes facilitating the misuse of deposit/savings accounts ········ - 57 -

[Topic] APG Yearly Typologies Report 2024 ········ *- 59 -*

4. Suspicious Transaction Report (STR) ········ - 60 -

(1) Overview and Reporting Status ········ - 60 -

(2) Examples of STR Utilization ········ - 62 -

(i) Examples of Cleared Cases Detected through STRs by the Prefectural Police

(ii) Examples of Cases in Which Investigating Authorities Other than the Prefectural Police Utilized STRs

[Recent Crime Cases and Trends Reported by Public Prosecutors Office] ········ *- 67 -*

[Recent Crime Cases and Trends Reported by National Tax Agency] ········ *- 68 -*

[Recent Crime Cases and Trends Reported by Japan Customs] ········ *- 69 -*

[Recent Criminal Cases and Trends Reported by Narcotics Control Department, Regional Bureaus of Health and Welfare, Ministry of Health, Labour and Welfare] ········ *- 70 -*

[Recent Crime Cases and Trends Reported by the Japan Coast Guard] ···· *- 70 -*

Section 4. Risk of Transaction Types, Countries/Regions, and Customer Attributes ···· ***- 71 -***

1. Transaction Types ···· **- 71 -**

(1) Non-Face-to-face Transactions ···· - 71 -

(i) Factors that Increase Risks

(ii) Trends of STRs

(iii) Measures to Mitigate Risks

(iv) Assessment of Risks

[Topic] Fraudulent Transfers, Online and Telephone Fraud, Investment/Romance Frauds via Social Media Using Online Banking ···· *- 76 -*

(2) Cash Transactions ···· - 78 -

(i) Factors that Increase Risks

(ii) Trends of STRs

(iii) Measures to Mitigate Risks

(vi) Assessment of Risks

(3) Cross-border Transactions ···· - 83 -

(i) Factors that Increase Risks

(ii)Notification of STRs

(ii) Measures to Mitigate Risks

(iv) Assessment of Risks

[Topic] Analysis of Trade-Based Money Laundering (TBML) ···· *- 92 -*

[Topic]Threats of International Fraud and ML Based in Southeast Asia ···· *- 93 -*

2. Countries/Regions ···· **- 94 -**

(1) Factors that Increase Risks ···· - 94 -

(i) North Korea

(ii) Iran

(iii) Myanmar

(2) Measures to Mitigate Risks ···· - 95 -

(3) Assessment of Risks ···· - 95 -

[Topic] Changes in Countries/Regions for Which the FATF Requested Its Members countries/regions to Apply Countermeasures in the FATF Statements or Designated as under the FATF's Monitoring Process to Improve AML/CFT Measures ···· *- 97 -*

3. Customer Attributes ···· **- 99 -**

(1) Boryokudan ···· - 99 -

(i) Factors that Increase Risks

(ii) Trends of STRs

(iii) Measures to Mitigate Risks

(iv) Assessment of Risks
(2) Non-resident Customers - 103 -
(i) Factors that Increase Risks
(ii) Measures to Mitigate Risks
(iii) Assessment of Risks
(3) Foreign Politically Exposed Persons - 104 -
(i) Factors that Increase Risks
(ii) Measures to Mitigate Risks
(iii) Assessment of Risks
(4) Legal Persons (Legal Persons without Transparency of Beneficial Owner) - 106 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Assessment of Risks
[Topic] Analysis of Criminal Groups Engaged in ML Using Corporations *- 113 -*
[Topic] Risk of the Misuse of Legal Arrangements for ML/TF *- 116 -*

Section 5. Risk of Products and Services ***- 118 -***

1. Major Products and Services in which Risk is Recognized - 118 -
(1) Products and Services Dealt with by Deposit-taking Institution - 119 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(2) Insurance Dealt with by Insurance Companies, etc. - 134 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(3) Products and Services Dealt with by Financial Instruments Business Operators, etc., and Commodity Derivatives Business Operators - 139 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks

(4) Trust Dealt with by Trust Companies, etc. - 145 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(5) Money Lending Dealt with by Money Lenders, etc. - 149 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risk
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(6) High-Value Electronically Transferable Prepaid Payment Instruments Dealt with by Issuers - 153 -
(i) Factors that Increase Risks
(ii) Measures to Mitigate Risks
(iii) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(iv) Assessment of Risks
(7) Funds Transfer Services Dealt with by Funds Transfer Service Providers - 157 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(8) Electronic Payment Instruments Dealt with by Electronic Payment Instruments Service Providers - 163 -
(i) Factors that Increase Risks
(ii) Measures to Mitigate Risks
(iii) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(iv) Assessment of Risks
(9) Cryptoassets Dealt with by Cryptoassets Exchange Service Providers - 166 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(10) Foreign Currency Exchanges Dealt with by Currency Exchange Operators - 175 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(11) Financial Leasing Dealt with by Financial Leasing Operators ······ - 180 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(12) Credit Cards Dealt with by Credit Card Operators ······ - 183 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(13) Real Estate Dealt with by Real Estate Brokers ······ - 188 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(14) Precious Metals and Stones Dealt with by Dealers in Precious Metals and Stones ······ - 193 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(15) Postal Receiving Services Dealt with by Postal Receiving Service Providers ······ - 199 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks
(16) Telephone Receiving Services Dealt with by Telephone Receiving Service Providers ······ - 203 -
(i) Factors that Increase Risks
(ii) Trends of STRs
(iii) Measures to Mitigate Risks
(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of
(v) Assessment of Risks

(17) Telephone Forwarding Services Dealt with by Telephone Forwarding Service Providers ········· - 205 -

(i) Factors that Increase Risks

(ii) Trends of STRs

(iii) Measures to Mitigate Risks

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

(v) Assessment of Risks

(18) Legal/Accounting Services Dealt with by Legal/Accounting Professionals ········· - 210 -

(i) Factors that Increase Risks

(ii) Measures to Mitigate Risks

(iii) Assessment of Risks

2. Products and Services That Should Be Monitored Closely ········· - 218 -

(1) Casinos ········· - 218 -

Section 6. Low-risk Transactions ········· - 220 -

1. Factors that Mitigate Risks ········· - 220 -

2. Types of Low-risk Transactions ········· - 221 -

Section 7. Risk Related to Terrorist Financing ········· - 224 -

1. Factors that Increase Risks ········· - 224 -

(1) International Terrorism Situation and Threat Targeting Japan ········· - 224 -

(2) Characteristics ········· - 226 -

(3) Domestic Cases ········· - 226 -

(4) Cases in foreign countries ········· - 227 -

2. Trends of STRs ········· - 228 -

(1) Key Points to Note When Submitting STRs ········· - 228 -

(2) Trends Observed in Reported Cases ········· - 229 -

3 Measures to Mitigate Risks ········· - 229 -

(1) Statutory measures ········· - 229 -

(2) Other Measures ········· - 231 -

4 Assessment of Risks ········· - 231 -

[Topic] Risk of Abuse of Nonprofit Organizations for TF ········· - 233 -

Introduction

The threat of money laundering and terrorist financing (hereinafter referred to as "ML/TF") in Japan is intensifying due to an increase in online and telephone fraud, and investment/romance fraud via social media, including those perpetrated from hideouts overseas for both types of fraud, the diversification of cyber crimes, and the spread of highly anonymous fund transfers using cryptoassets, etc.

The international community is strongly calling for the development and implementation of effective, risk-based countermeasures through the FATF (Financial Action Task Force) recommendations and mutual evaluations among participating countries.

The Government of Japan established the "Inter-Ministerial Council for AML/CFT/CPF Policy" (hereinafter referred to as the "Inter-Ministerial Council") in August 2021, and in May 2022, the Inter-Ministerial Council decided on the "Strategic Policy towards Promoting AML/CFT/CPF" (hereinafter referred to as the "Strategic Policy"), outlining four pillars to focus on: 1) Full implementation of risk-based approach, 2) Swift responses to new technologies, 3) Strengthening international cooperation and coordination, and 4) Enhancing inter-agency coordination and public-private partnership. The Inter-Ministerial Council, looking ahead to the Fifth Round of Mutual Evaluation of Japan by the FATF, also formulated a new "National AML/CFT/CPF Action Plan (FY2024-26)" in April 2024 to further enhance the effectiveness of AML/CFT measures and to respond to changes in risks environment.

Furthermore, in recent years, the Financial Services Agency, the National Police Agency, and financial institutions have been steadily building a framework for strengthening countermeasures through collaboration between the public and private sectors, including advancing practical-level information sharing and discussions on appropriate countermeasures against non-face-to-face investment/romance fraud via social media, where the increase in losses has become particularly pronounced.

Not only to meet international demands, but also as an effective measure to protect national assets, it is necessary to further advance these efforts.

The National Risk Assessment-Follow-up Report (hereinafter referred to as the "NRA-FUR") is prepared by the National Public Safety Commission with the cooperation of relevant ministries and agencies, and private sector. It is published annually to ensure timely and appropriate identification and analysis of the risks of ML/TF in Japan, which are constantly evolving in line with changes in social conditions and criminal tactics, thereby contributing to a risk-based approach.

To effectively prevent the transfer of criminal proceeds and terrorist financing it is essential that relevant parties, including competent authorities and specified business operators, fully understand the risks of ML/TF and their respective roles, and work together in a public-private partnership to implement countermeasures.

This NRA-FUR aims to promote an appropriate understanding of the risks of ML/TF among relevant parties and to support the development of effective countermeasures commensurate with those risks, thereby ensuring the soundness of financial system in Japan and safety of citizen's lives and contributing to the sustainable development of economic activities.

[Overview of the NRA-FUR 2025]

1. Risk Assessment Method

The NRA-FUR is published annually pursuant to the provisions of Article 3, paragraph (3) of the Act on Prevention of Transfer of Criminal Proceeds. Based on the contents of the “National Risk Assessment-Baseline Analysis” published in 2014, the National Public Safety Commission has continued to publish this report annually since 2015, and it is positioned as the foundational basis for the risk-based approach adopted by specified business operators. The risk assessment in the NRA-FUR is conducted using Japan-specific methods, referencing the FATF guidance on risk assessment.

2. Environment Surrounding Japan

(1) Geographic, social, and economic environment

Japan is an island country, and traffic and logistics to and from other countries are conducted via the sea and airports. While the total population is on a long-term downward trend due to the declining birthrate, the number of foreign residents is on the rise. Japan also has a highly developed financial sector, and access to financial services is widely ensured through the nationwide network of financial institution branches and ATMs. While the cash balance in circulation remains high compared to other countries, the proportion of cashless payments is steadily increasing.

(2) Criminal environment

Of all criminal offences in 2024, the amount of losses caused by offences against property accounted for approximately 402.1 billion yen, surpassing the level recorded in 2002, the highest since 1989. In particular, the amount of losses caused by frauds reached approximately 307.5 billion yen, and the situation remains serious. The amount of losses caused by online and telephone frauds amounted to 71.88 billion yen, and the amount of losses caused by investment/romance frauds via social media amounted to 127.19 billion yen, both of which were record highs. Regarding threats in cyberspace, the number of reported phishing cases reached approximately 1.72 million in 2024, continuing its upward trend, and the amount of losses caused by credit card frauds reached a record high of approximately 55.5 billion yen. Losses from ransomware also remained at a high level, and in 2024, a case was confirmed in which a cyber-attack group backed by North Korea stole cryptoassets worth approximately 48.2 billion yen from a domestic cryptoassets exchange service provider.

3. Analysis of Money Laundering Cases

(1) Offenders

The primary offenders involved in ML in Japan include “anonymous and fluid criminal groups,” “Boryokudan” and “crime groups of foreigners in Japan.” In particular, anonymous and fluid criminal groups, whose core members remain anonymous and whose crime actors become fluid through recruitment via social media and other means, employ diverse ML methods for the criminal proceeds they acquire. Revenue-generating activities by anonymous and fluid criminal groups encompass a wide range of offences, including online and telephone frauds, investment/romance frauds via social media, organized theft, revenue-generating activities in entertainment districts, and online gambling offences. Furthermore, a structure is observed where the core of the organization profits by recirculating the proceeds, such as using funds acquired through crime for new revenue-generating activities. Additionally, cases have been confirmed where some of these funds appear to flow to Boryokudan, and where members of Boryokudan are involved as leaders or members of anonymous and fluid criminal groups.

(2) Predicate offences

The number of cleared cases of ML offences in 2024 totaled 1,283 cases, combining violations of the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act, and is on the upward trend due to enhanced police crackdowns and other factors. In the total number of cleared cases by predicate offences over the past three years, fraud and computer fraud accounted for approximately 50%, with an increase of cleared cases related to online and telephone frauds and investment/romance frauds via social media.

(3) Major transactions misused for money laundering

Over the past three years, products and services dealt with by deposit-taking institutions accounted for approximately 60% of transactions misused for ML. In recent years, the misuse of credit cards has increased, while misuse of prepaid payment instruments, cryptoassets, and funds transfer services has also been observed.

(4) Suspicious transaction report (STR)

Against the backdrop of heightened awareness nationwide regarding AML/CFT, the number of STRs are on the upward trend. The annual number of STR notified to the National Police Agency in 2024 reached approximately 850,000 cases.

4. Risk of Transaction Types, Countries/Regions and Customer Attributes

(1) High-risk transaction types

(i) Non-face-to-face transactions

Since it is not possible to directly verify the counterparty or identification documents, compared to face-to-face transactions, it is easier to open accounts under the names of fictitious or other parties by falsifying identification matters through the forgery or alteration of identification documents. There is also a risk that a third party other than the contract holder may conduct a transaction after the completion of the verification at the time of transaction. In fact, transfers via online banking have become one of the methods for delivering stolen funds in cases of online and telephone frauds and investment/romance frauds via social media, and cases of accounts being opened using forged documents have been confirmed.

(ii) Cash transactions

In addition to its high anonymity, it often makes it difficult for investigating authorities to trace fund transfers, making it susceptible to misuse for ML/TF money laundering and similar purposes. While the use of cash is on the declining trend due to the rise in the proportion of cashless transactions, there are still cases where cash transactions are misused.

(iii) Cross-border transactions

Compared to domestic transactions, it often makes it difficult for investigating authorities to trace fund transfers, and in recent years, funds have been transferred overseas using a variety of means, including cryptoassets. Fund transfers to foreign countries by “anonymous and fluid criminal groups” have also been confirmed.

(2) High-risk countries/regions

Based on the FATF statement, the Act on Prevention of Transfer of Criminal Proceeds and its Enforcement Order stipulates that Iran and North Korea are jurisdictions deemed to have inadequate AML/CFT systems. Furthermore, transactions with Myanmar fall under the category of “those that are deemed to have high risk of ML/TF according to the level of risks prescribed in the NRA-FUR under the Ordinance of Enforcement of the Act on the Prevention of Transfer of Criminal Proceeds.

3. High-risk Customer Attributes

(i) Boryokudan

It is a representative form of organized crime in Japan that intend to gain profit in organized manners.

(ii) Non-resident customers and foreign politically exposed persons (Foreign PEPs)

CDD measures to verify identification matters and other information are restrictive, making CDD difficult.

(iii) Legal persons (Legal persons without transparency of beneficial owners, etc.)

Legal persons have the characteristic of such as high transactional credibility and the ability to transfer large amounts of funds through legal persons’ accounts. There have been cases where this characteristic has been exploited, with third parties taking control of companies’ accounts through the establishment of shell companies or the acquisition of inactive companies, and using these accounts to conceal or transfer criminal proceeds obtained through online and telephone frauds, investment/romance fraud via social media, the operation of online casinos, etc.

5. Risk of Products and Services

Taking into consideration a comprehensive range of factors, including the criminal environment related to online and telephone frauds, investment/romance fraud via social media, cyber crimes, the offenders involved in ML and the products and services misused in predicate offences, high-risk transaction type such as non-face-to-face transactions, cash transactions, and cross-border transactions, the scale of each business type, and the vulnerabilities of each products and services, products and services dealt with by deposit-taking institution, cryptoassets, funds transfer services and electronic payment instruments are recognized as a relatively higher risk than other business types.

6. Low-Risk Transactions

Factors that mitigate risks include the transparency of the source of funds, etc. Additionally, types of low-risk transactions include certain transactions in money trusts, etc.

7. Risk Concerning Terrorist Financing

The risk of terrorist financing in Japan is assessed to be relatively low compared to other countries. There have been no terrorist acts carried out in Japan by terrorists designated by the United Nations Security Council so far. However, the possibility of funds being collected in that country and being remitted abroad should not be excluded, and transactions with individuals suspected of having ties to Islamic extremists are recognized as having a particularly high risk of terrorist financing.

[Overview of Assessment]

Threat		Vulnerability
Offenders	Predicate offences (fraud, theft, etc.)	Major transactions misused for money laundering (deposit/savings accounts, domestic exchange transactions, etc.)
1. Anonymous and fluid criminal groups 2. Boryokudan 3. Crime groups of foreigners in Japan		

○ **Risk Assessment (1): High-risk transaction types, countries/regions and customer attributes**

Vulnerability: Transaction types	Countries/Regions	Customer Attributes
1. Non-face-to-face transactions 2. Cash transactions 3. Cross-border transactions	1. Countries/regions where the implementation of countermeasures is requested by the FATF statements Iran, North Korea 2. Countries/regions required to apply enhanced CCD measures commensurate with the risks arising from countries/regions designated by the FATF statement Myanmar	1. Boryokudan 2. Non-resident customers 3. Foreign Politically Exposed Persons (Foreign PEPs) 4. Legal persons (Legal persons without transparency of beneficial owners, etc.)

○ **Risk Assessment (2): Products and Services**

Products and Services	
Relatively higher risk than other business forms	● Products and services dealt with by deposit-taking institution (excluding those listed below) ● Funds transfer services ● Electronic payment instruments ● Cryptoassets
Transactions considered to be of risk	● Insurance ● Investment ● Trust ● Money lending ● Foreign currency exchanges ● Financial leasing ● Credit card ● Real estate ● Precious metals and stones ● Postal receiving services ● Telephone receiving services ● Telephone forwarding services ● High-value electronically transferable prepaid payment instruments ● Legal/Accounting services

○ **Low-risk transactions (transactions which simplified CDD stipulated in Article 4 of the related Ordinance of the Act on Prevention of Transfer of Criminal Proceeds is permitted)**

Factors that mitigate risks
1. Source of funds is identified 2. The customer, etc., is the national government or a local public entity 3. The customers, etc., are limited under laws and regulations 4. The transaction process is supervised by the national government, etc. based on laws, etc. 5. It is difficult to disguise the actual status of legal persons, etc. 6. Minimal or no fund-accumulation features 7. The transaction amount is less than the regulatory threshold 8. Customer identification measures are secured by laws, etc.

○ **Risk concerning terrorist financing**

Threat	Vulnerability
Terrorist organizations, including Islamic extremists such as ISIL and AQ, and those involved in terrorist financing	Legal and illegal sources and means of terrorist financing

Section 1. Risk Assessment Method

1. History

In modern society, where information technology and globalization of economic/financial services are advancing, the state of ML/TF is changing rapidly. In order to strongly cope with the problem, global countermeasures are required through the cooperation of countries.

In Recommendation 1 of the 40 Recommendations revised in February 2012 (hereinafter referred to as the "FATF Recommendations"), the FATF made a series of requests to countries, including a request to identify and assess money laundering*[1] and terrorist financing*[2] risks for the country*[3].

In addition, in the G8 Lough Erne Summit held in June 2013, in light of the situation in which companies etc. with non-transparent ownership/control structures were being used for money laundering and tax avoidance, "the G8 Action Plan Principles to Prevent the Misuse of Corporations and Legal Arrangements" (hereafter referred to as the "G8 Action Plan Principles") were agreed on which stipulated, among other things, that each country should understand the risks to which their anti-money laundering and countering the financing of terrorism regime is exposed, and implement effective and proportionate measures to target those risks.

In the same month, in accord with the FATF Recommendations and the G8 Action Plan Principles, Japan set up a working group, which consisted of the National Police Agency and other relevant ministries and agencies, including the Financial Services Agency, to assess the degree of ML/TF risks in transactions (hereinafter referred to as "risk(s)"), and in December 2014, the National Risk Assessment-Baseline Analysis (hereinafter referred to as the "NRA-Baseline Analysis") was published*[4].

Since then, pursuant to the provisions of Article 3, paragraph (3) of the Act on Prevention of Transfer of Criminal Proceeds*[5] which were newly established when the act was revised in 2014, the National Public Safety Commission has prepared and published NRA-FUR, that describes risks, etc. in each category of the transactions carried out by specified business operators*[6], etc. in keeping with the contents of the NRA-Baseline Analysis.

---

*1 In general, money laundering refers to an act of concealing the sources or real owners of criminal proceeds in an attempt to prevent investigating authorities from discovering the proceeds or clearing the case. In Japan, money laundering is prescribed as an offence in the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act.

*2 Money laundering and terrorist financing differ in the following respects, among others: (i) terrorist financing does not always involve funds obtained by illegal means; (ii) transactions related to terrorist financing could be smaller in amount than those related to money laundering; and (iii) the countries/regions that require attention as remittance destinations may be different between money laundering and terrorist financing. The NRA-FUR describes risks based on these differences. In addition, because terrorist financing itself is a crime and terrorist funds themselves can be criminal proceeds subject to money laundering, it is considered that those who try to finance terrorists attempt to conceal the transfer of funds, like other criminal proceeds, by misusing various transactions and products/services. Thus, the risks in transactions and products/services described in the NRA-FUR include terrorist financing risks.

*3 In October 2020, FATF Recommendation 1 was revised, adding the proliferation financing risk, which refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7, to the scope of risk assessment. In Japan, the Policy Council published the "National Risk Assessment of Proliferation Financing in Japan (First Edition)" in March 2024 and updated it in December of the same year. The subject of the NRA-FUR does not include proliferation financing risk.

*4 The NRA-Baseline Analysis stated that "At the national level, relevant ministries and agencies will take strategic and effective measures according to the result of risk assessment, based on the risk-based approach."

*5 The Article provides that the National Public Safety Commission shall each year conduct investigation and analysis of the modus operandi and other circumstances of the transfer of criminal proceeds to prepare and publish a National Risk Assessment-Follow-up Report, which reports the results of the investigation and analysis, including the risk of transfer of criminal proceeds, for each category of transactions carried out by specified and other business operators.

*6 Meaning the persons listed in each item of Article 2.2 of the Act on Prevention of Transfer of Criminal Proceeds.

2. Purpose

The purpose of the NRA-FUR is to identify and assess the risks of specific types of transactions conducted by specified business operators being misused for ML/TF. Specified business operators are required to take into consideration the contents of the NRA-FUR, determine whether there is any suspicion of ML/TF, and submit suspicious transaction report (STR)[*1], as well as take measures to properly conduct verification at the time of transaction, etc.[*2*3], in order to effectively prevent the products and services they handle from being misused for the transfer of criminal proceeds. The NRA-FUR serves as the premise for effective and efficient AML/CFT (Anti-Money Laundering and Countering the Financing of Terrorism) measures based on a risk-based approach taken by specified business operators.

In addition to referring to the NRA-FUR, it is necessary to take into account the contents of the guidelines issued by the authorities that supervise specified business operators (hereinafter referred to as the “competent authorities”), and it is also considered useful to refer to publications such as reports and annual reports on the ML/TF risks and AML/CFT measures issued by the competent authorities, etc[*4]. For information on the main history of Japan’s AML/CFT measures, legal systems related to AML/CFT measures, international cooperation, etc., it is recommended to refer to the “Annual Report” published by the National Police Agency.

3. Assessment Method

(1) Assessment Method

The National Public Safety Commission, which is in a position to collect, organize, and analyze information related to the transfer of criminal proceeds and suspicious transactions, has obtained information from competent authorities and industry associations, regarding the characteristics of products and services handled by specified business operators and the status of their AML/CFT measures, and has prepared the NRA-FUR utilizing the information and expertise it possesses.

The NRA-FUR takes into account the contents of the NRA-Baseline Analysis[*5] published in 2014, and has been published annually since 2015, updating and expanding the scope of survey and analysis in its preparation process in response to changes in the risks of ML/TF surrounding Japan. In the NRA-FUR, the risk factors, namely “threats” and “vulnerabilities,” are identified as shown in the following table. It is based on the “National Money Laundering

---

*1 Article 8, paragraph (3) of the Act on Prevention of Transfer of Criminal Proceeds

*2 Article 11, paragraph (1), item (iv) of the Act on Prevention of Transfer of Criminal Proceeds

*3 Article 32, item (i) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds provides that “Specified business operators shall investigate and analyze the transactions they conduct, and prepare documents or electromagnetic records that describe or record the results of the investigation and analysis, including the degree of risk of the transfer of criminal proceeds arising from such transactions (hereinafter referred to as “their AML/CFT Risk assessment documents”), and shall review and make necessary changes as necessary.”

*4 Financial Service Agency “‘Anti-Money Laundering, Counter Financing of Terrorism, Counter-Proliferation Financing, and Counter Financial Crimes’ Current Status and Challenges (June 2025)”; National Police Agency “Annual Report,” “The White Paper on Police,” “Situation of organized crime”; Ministry of Justice “White Paper on Crime,” etc.

*5 In the NRA-Baseline Analysis, the subcommittee conducted a multifaceted and comprehensive analysis to assess the risks, based on the following documents and statistics: (i) FATF guidance (National Money Laundering and Terrorist Financing Risk Assessment), the FATF Recommendations, and findings in the 3rd round of mutual evaluation of Japan by the FATF, (ii) various statistics and case studies collected by the subcommittee from relevant ministries and agencies regarding the actual situation of ML/TF and countermeasures against them, (iii) written questionnaires or interview surveys conducted through competent authorities on industry associations and businesses regarding their efforts on AML/CFT and their recognition of the vulnerability to ML/TF of their own transactions and the products and services they handle, (iv) status of suspicious transaction reports and cleared cases of money laundering offences (qualitative and quantitative), (v) opinion hearings and public comments from external experts (finance and economics scholars, banking practitioners, and experts with knowledge of AML/CFT), and (vi) research on risk assessment in other countries.

and Terrorist Financing Risk Assessment" (February 2013) published by the FATF[*1], and also takes into consideration the FATF Recommendations, the Interpretive Notes[*2], findings in the 3rd and 4th Rounds of Mutual Evaluation of Japan by the FATF, cleared cases of ML identified by law enforcement agencies, the results of analysis of STRs, information on specified business operators identified by competent authorities, and measures under the Act on Prevention of Transfer of Criminal Proceeds.

Threat	Offenders: Anonymous and fluid criminal groups, Boryokudan, and Crime groups of foreigners in Japan Predicate offences[*3]: Fraud, Theft, etc., that generate criminal proceeds
Vulnerability	Products and services such as deposit/savings accounts and domestic exchange transactions Transaction types including non-face-to-face transactions and cash transactions, etc.

In addition, as the "consequence," volume of criminal proceeds to be transferred, risks of supporting or facilitating organized crimes, impact on sound economic activities, etc., were considered to identify risk factors[*4] in terms of transaction types, countries/regions, customer attributes, and products/services.

Regarding each risk factor, the following information was analyzed to assess risks in a multifaceted and comprehensive manner.

- Inherent risks of being misused for ML/TF
- ML cases
- Reporting status of STRs
- Status regarding risk mitigation measures (obligations of specified business operators under laws and regulations, guidance and supervision of specified business operators by competent authorities and voluntary efforts made by industry associations or specified business operators, etc.)

---

*1 Although the Guidance expresses the view that there is no universal ML/TF risk assessment method, for a general understanding, it does show the following as risk factors and an assessment process.
Risk can be seen as a function of three factors: threat (a person or group of people, object or activity with the potential to cause harm to the state, society, the economy, etc.), vulnerability (things that can be exploited by the threat or that may support or facilitate its activities), and consequence (the impact or harm that ML/TF may cause to the economy and society). However, given the challenges in determining or estimating the consequences, it may be acceptable to focus primarily on understanding threats and vulnerabilities. In addition, the assessment process can generally be divided into the following three stages: (i) Develop an initial list of potential risks or risk factors to be analyzed, drawn from known or suspected threats or vulnerabilities. New or previously undetected risks may also be identified afterward (identification stage). (ii) Conduct the analysis on the identified risks or risk factors taking into account the nature, likelihood, etc. (analysis stage). (iii) Determine priorities for addressing the risks (evaluation stage).

*2 As examples of situations that increase the ML/TF risks, the Interpretive Note to Recommendation 10 (Customer Due Diligence) cites non-resident customers, legal persons or legal arrangements that are personal asset-holding vehicles, businesses that are cash-intensive, the ownership structure of the company that appears unusual or excessively complex, countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems, non-face-to-face business relationships or transactions, etc.

*3 Predicate offences are described in "2. Predicate Offences" of "Section 3: Analysis of Money Laundering Cases" of this NRA-FUR.

*4 In addition to them, factors that increase the risks include the scales of business operators. As the number and volume of transactions increase, it becomes more difficult to identify and trace criminal proceeds in the transactions. Because of this, among other reasons, larger business operators are generally considered to present higher risks. In response, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to strive to develop necessary systems, including conducting employee education and training, to fulfill the obligation to accurately perform verification at the time of transaction, etc., and it seeks to reduce the risks through the development of systems commensurate with the scales of the specified business operators.

(2) Information Used in the Assessment

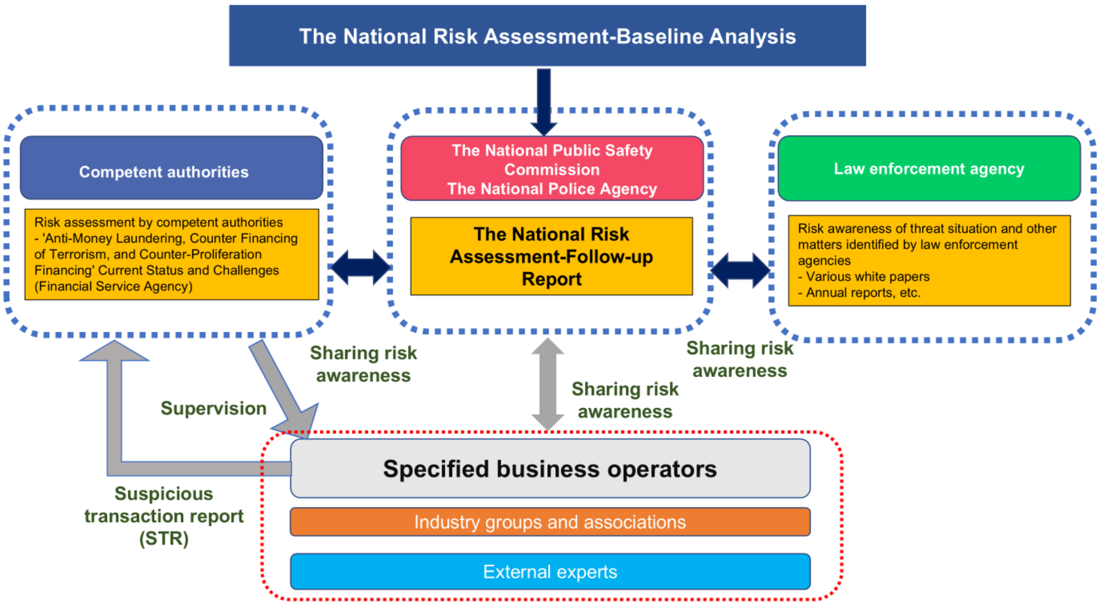
For the assessment, the following information, which was collected widely while making efforts to promote close collaboration between the relevant ministries and agencies, law enforcement agencies, industry associations, specified business operators and experts with expertise in AML/CFT, was used for analysis.

- Statistics, knowledge, cases, and risk awareness held by relevant ministries and agencies and law enforcement agencies
- Information on cleared cases of ML and STRs over the past three years held by the National Public Safety Commission
- Information on the level of awareness of and the status of AML/CFT measures as grasped by the competent authorities or obtained through exchanges of opinions with industry associations, specified business operators, and experts with knowledge of AML/CFT
- Information collected by the relevant ministries and agencies through exchanges of opinions with authorities of other countries (including regions, the same applies hereinafter) in the scheme of international cooperation
- Guidances and reports related to risk analysis and supervision using a risk-based approach published by the FATF
- Reports and statistics published by international organizations, such as Egmont Group, Asia/Pacific Group on Money Laundering (APG), International Criminal Police Organization (ICPO), United Nations Office on Drugs and Crime (UNODC), World Bank, International Monetary Fund (IMF), etc.

The annual publication of the NRA-FUR serves as a mechanism for appropriately grasping changes in the ML/TF risks surrounding Japan. In addition to analyzing risks specific to Japan, external risks are analyzed, including transactions that utilize new technologies, taking into account global trends in predicate offences and ML/TF.

The NRA-FUR is available on the websites of the National Public Safety Commission and the Japan Financial Intelligence Center (JAFIC).

Table 1: Relationship diagram for preparing the NRA-FUR



4. Updates to the NRA-FUR

(1) Major Updates to the NRA-FUR up to Last Year

Month and year of publication	Main items that have been changed or expanded since the prior year's NRA-FUR
September 2015	● Expanded the analysis scope of products and services in which risk is recognized to include all the transactions conducted by specified business operators under the Act on Prevention of Transfer of Criminal Proceeds (added money lending, financial leasing, credit cards, telephone receiving services, and telephone forwarding services)
November 2016	● Added "virtual currency handled by virtual currency exchangers" to products and services in which risk is recognized ● Added "international terrorists (Islamic extremists, etc.)" to customer attributes of high-risk transactions
November 2017	● Excluded "transactions with customers who use non-photo identification" from the list of high-risk transactions
December 2018	● Added descriptions of specific examples of efforts by business operators and modus operandi of ML cases ● Added descriptions regarding casinos
December 2019	● Added examples of cases in which arrests were made as a result of STRs
November 2020	● Added descriptions regarding environment surrounding Japan ● Expanded descriptions regarding risk mitigation measures taken by competent authorities, industry associations, or specified business operators
December 2021	● Added descriptions of cyber crimes and international situation of cryptoassets ● Expanded descriptions of cases regarding legal persons without transparency, funds transfer services, and cryptoassets ● Introduced the FATF report on illegal wildlife trade
December 2022	● Added descriptions regarding risk of abuse of NPOs for TF ● Added descriptions regarding new threats and vulnerabilities identified by competent authorities ● Added information on the use of STRs by law enforcement agencies other than the police ● Introduced an FATF report on environmental crimes
December 2023	● Added "electronic payment instruments dealt with by electronic payment instruments service providers" to products and services in which risk is recognized ● Expanded description of recent situation concerning online and telephone fraud ● Introduced an FATF report on ransomware
November 2024	● Changed "online and telephone fraud group" among the offenders in ML to "anonymous and fluid criminal groups" and added descriptions regarding revenue-generating activities such as investment/romance fraud via social media ● Deepened the analysis of legal persons in light of the fact that shell companies or opaque companies and corporate accounts are being misused for ML ● Introduced reports by international organizations such as APG, FATF, and UNODC on cyber-related fraud (CEF) and online casinos

(2) Major Changes in NRA-FUR in Light of Recent Changes in Situations

The 2025 NRA-FUR has been updated and enhanced to reflect changes in the domestic and international situations, the results of the FATF's 4th Round of Mutual Evaluation, and responses toward the 5th Round of Mutual Evaluation. The main changes are as follows:

(i) Regarding the offenders in ML, the traditional order has been revised in light of the criminal environment and its impact on sound economic activities, with "anonymous and fluid criminal groups" now listed at the top, and the descriptions regarding revenue-generating crimes have been updated.

(ii) Based on the actual situation in which online casinos are accessed from within Japan and the actual status that ML is conducted utilizing online casino system, the survey results on the actual status, measures taken by competent authorities and specified business operators, and the flow of funds related to online casinos and other matters are described.

(iii) In light of the fact that legal person and corporate deposit/savings accounts are being misused for ML by criminal groups specializing in ML, the analysis of cases of misuse has been deepened.

(iv) Descriptions on non-face-to-face transactions, which are considered to be high-risk transactions, has been updated, and a topic on online banking has been added.

(v) Descriptions on cross-border transactions, which are considered to be high-risk transactions, have been updated, and a topic on Trade-Based Money Laundering (TBML) and threat of fraud based in Southeast Asia.

(vi) To clarify descriptions regarding the risk concerning terrorist financing, it has been organized as a separate chapter.

Section 2. Environment Surrounding Japan

This section describes the geographic, social, economic and criminal environments that constitute the premise of risk assessment of ML/TF in Japan. The geographic, social, economic environments primarily constitute a factor related to vulnerabilities susceptible to be misused for ML/TF, while the criminal environment primarily constitutes a factor related to threat of ML/TF.

1. Geographic environment

Japan is an island country located in the eastern part of the Eurasian Continent, in a region called Northeast Asia (or East Asia), and surrounded by the Pacific Ocean, the Okhotsk Sea, the Sea of Japan, and the East China Sea, with a total territory of approximately 378,000 square kilometers. Traffic and logistics to and from other countries are conducted via the sea and airports. At seas and airports nationwide, immigration control and customs procedures are conducted from the viewpoints of preventing terrorism and smuggling committed by international crime groups , etc.

2. Social environment

The total population of Japan as of October 1, 2024, was approximately 123.80 million, marking 14 consecutive years of decrease. The ratio of the population aged 65 and over to the total population reached a record high of 29.3%, which is higher than in other developed countries. The population of Japan is in a long-term decline and is estimated to fall below 100 million by 2056.

The number of foreigners entering Japan*[1] in 2024 was approximately 36.78 million. This represents a significant increase from the previous year's approximate 25.83 million, marking a record high. The total number of new entrants was approximately 34.02 million. As far as the number of new entrants by nationality and region is concerned, the number of persons from South Korea was the largest, followed by from Taiwan and China*[2]. Regarding the purpose of entry (status of residence), the number of Temporary Visitors was the largest at approximately 33.36 million (98.1%), followed by Student at approximately 170,000 (0.5%), and foreigners with the residence statuses of Technical Intern Training at approximately 150,000 (0.4%), respectively.

The number of foreign residents as of the end of 2024 was approximately 3.77 million, 10.5% more than the previous year. In terms of the number of foreign residents by nationality and region, China was the largest and accounted for 23.2% of the total, followed by Vietnam, South Korea, the Philippines, and Nepal.

3. Economic environment

The Japanese economy occupies a vital position in the world economy. The nominal GDP in 2024 (Quarterly Estimates of GDP for Apr.-Jun. 2025 (The Second Preliminary Estimates)) was 608.4 trillion yen, the fourth-largest economy after the United States, China, and Germany. The real GDP growth rate in FY2024 was 0.7%. The share of nominal gross value added by economic activity (industry) in 2023 was 0.9% for the primary industry, 26.1% for the secondary industry, and 72.9% for the tertiary industry. Regarding the trade value in 2024, Japan's exports amounted to 107.879 trillion yen, and imports amounted to 112.5591 trillion yen. Japan's main export partners were the United States, China, South Korea, Taiwan, Hong Kong, and its import partners were China, the United States, Australia, the United Arab Emirates, South Korea.

In Japan, cross-border transactions are conducted freely. However, economic sanctions based on the FEFTA have been implemented in consideration of North Korea's missile launches and nuclear tests, Iran's nuclear development and Russia's aggression against Ukraine, etc.

Besides, Japan has a highly developed financial sector as a global financial center. A considerable number of financial transactions are conducted as one of the world's leading international financial centers. The financial system

*1 The total number of new entrants and re-entrants. "The number of new entrants" refers to the number of individuals who have been granted residency status and permitted to land in Japan upon entry, while "re-entrants" are foreigners (including special permanent residents) who reside in Japan and have temporarily left Japan and then re-entered.

*2 In this NRA-FUR, "China" does not include "Taiwan," "Hong Kong Special Administrative Region" and "Macao Special Administrative Region," unless otherwise specifically stated. However, the number of foreign residents includes those who are from "Hong Kong Special Administrative Region" and "Macao Special Administrative Region."

is nationwide, and funds can be transferred quickly and reliably. As of the end of March 2024, the number of branch offices of major financial institutions*[1] was 37,181 (including 172 branch offices located abroad). There were 83,000 ATMs*[2] installed with ease of access to the financial system. Furthermore, 3 of the 29 global systemically important banks (G-SIBs) designated by the Financial Stability Board (FSB) in 2024 were Japanese financial institutions.

In terms of the scale of financial transactions in Japan, the balance of bank deposits at the end of March 2025 was approximately 1,190 trillion yen. As for settlement transactions in 2024, domestic exchange transactions comprised approximately 3,814 trillion yen (approximately 2.1 billion cases), with a daily average of about 16 trillion yen (approximately 8.61 million cases), and the amount of foreign exchange in settled in yen was approximately 6,044 trillion yen (approximately 8.39 million cases), with a daily average of about 25 trillion yen (approximately 34,000 cases).

Looking at the size of the securities market, as of the end of December 2024, the total market capitalization of stocks in Japan was approximately 996 trillion yen. During 2024, the trading value of listed stocks on the Tokyo Stock Exchange was about 1,255 trillion yen in the Prime Market, 35 trillion yen in the Standard Market, and 34 trillion yen in the Growth Market.

Regarding cash transactions, Japan has a higher cash circulation compared to other countries, due to a combination of factors including a high number of financial institution branches and ATMs, making it easy to withdraw and deposit cash from bank accounts, and the high level of anti-counterfeiting technology in banknotes, resulting in the minimal circulation of counterfeit bills. On the other hand, the ratio of cashless payments*[3] has been steadily increasing due to the promotion of cashless transactions.

Japan’s economic environment, which has been globalized and highly developed, provides various ML/TF means and methods to domestic and foreign people who intend to do ML/TF. Among the various transactions, products, and services globally, these people choose the most suitable means to conduct ML/TF.

4. Criminal environment

(1) Domestic Crime Situation

(i) Number of Recognized Criminal Offence Cases

Among the indicators measuring Japan’s criminal circumstances, the total number of recognized criminal offence cases had consistently decreased from 2003 to 2021. However, in 2024, there were 737,679 cases, increasing for the third consecutive year compared to the post-war record low in 2021 (an increase of 4.9% from the previous year) (see Table 2).

Among the criminal offence cases, the trend in the amount of losses from offences against property*[4] has increased by 59.6% from the previous year to approximately 402.1 billion yen. This exceeds the amount of losses in 2002, which was the highest since 1989. Looking at the breakdown of this figure, the amount of losses caused by fraud increased to 307.5 billion yen, a significant increase of 89.1% from the previous year, making the situation extremely alarming (see Table 3).

---

*[1] Here, the major financial institutions refer to city banks, regional banks, trust banks, second regional banks, SBI Shinsei Bank, Aozora Bank, and Japan Post Bank.

*[2] The total number of city bank, regional bank, trust bank and second regional bank ATMs was calculated as of the end of September 2024, and the number of Japan Post Bank ATMs was calculated as of the end of March 2024.
Note that this number does not include ATMs of SBI Shinsei Bank, Aozora Bank, and cooperative financial institutions, or ATMs of banks and other institutions that have their ATMs installed in convenience stores, etc. and primarily provide payment services.

*[3] The ratio of cashless payments to private final consumption expenditure. According to the calculations by the Ministry of Economy, Trade, and Industry, the cashless payment ratio in 2024 increased from 26.8% in 2019 to 42.8%.

*[4] Robbery, extortion, theft, fraud, embezzlement, and embezzlement of lost property

Table 2: Trends in the Number of Recognized Criminal Offence Cases

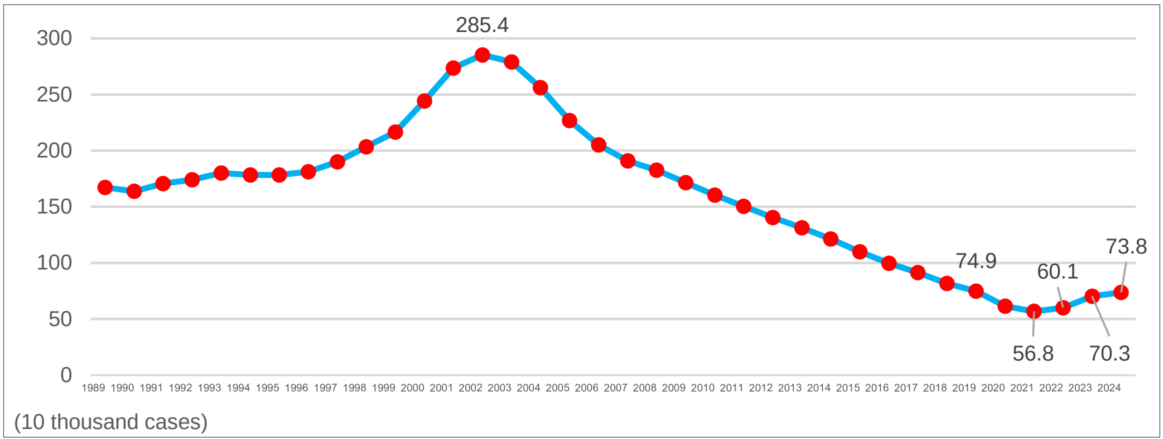
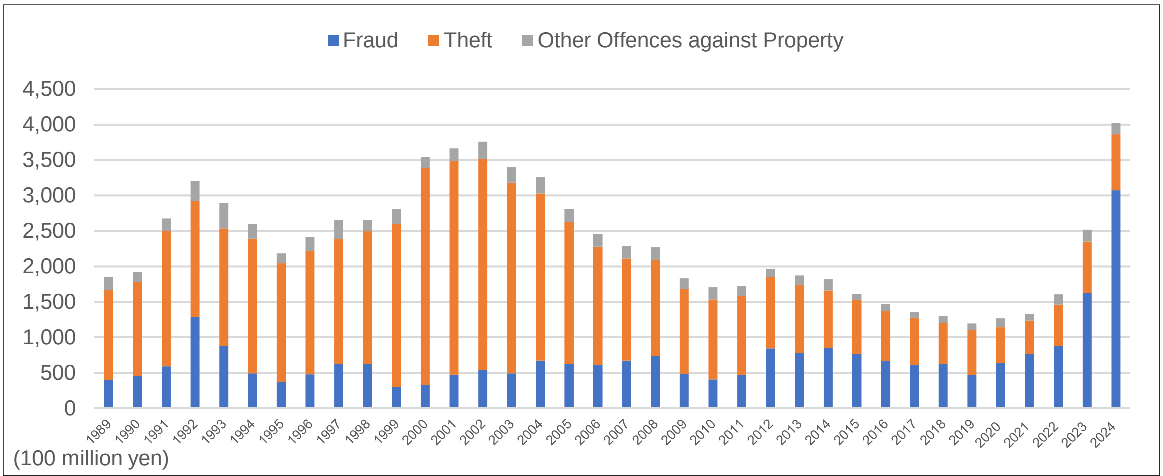


Table 3: Trends in the Amount of Losses from Offences against Property (Limited to Criminal Offences)



Amount of Losses (in 100 million yen)	2019	2020	2021	2022	2023	2024
Fraud	469.5	640.1	763.0	876.8	1,625.8	3,074.7
Theft	633.2	501.6	474.0	585.3	725.8	789.3
Other Offences against Property	90.6	125.3	89.5	145.8	167.4	156.6
Total	1,193.3	1,267.0	1,326.5	1,607.8	2,519.1	4,020.7

Note: As the figures are rounded to the nearest tenth, the total may not necessarily match the sum of the breakdown.

*(ii) Fraud (Online and Telephone Fraud[*1] and Investment/Romance Fraud Via Social Media [*2])*

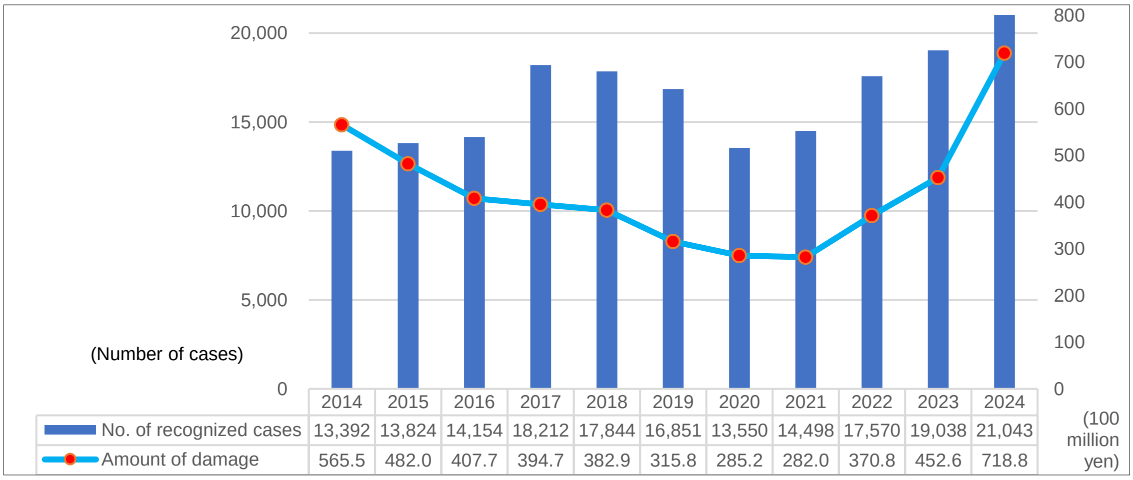
In 2024, the number of recognized online and telephone fraud cases was 21,043 cases and the amount of losses was 71.88 billion yen, both of which increased compared to the previous year. In particular, the amount of losses exceeded the previous record of 56.55 billion yen in 2014, indicating a continuing serious situation (see Table 4).

Losses was concentrated in major metropolitan areas, with the number of recognized cases totaling 3,494 in Tokyo, 2,644 in Osaka, 1,999 in Kanagawa, 1,586 in Saitama, 1,469 in Aichi, 1,445 in Hyogo, and 944 in Chiba, with these seven prefectures accounting for 64.5% of the total number of recognized cases. The average amount of losses per day was 196.39 million yen, and the average amount of losses per completed case was 3.503 million yen.

Looking at the status of the recognized cases by modus operandi, the number of recognized cases of "It's me" fraud was 6,752 cases and the amount of losses from the fraud was 45.84 billion yen, both of which increased. The figures accounted for 32.1% of the total number of recognized cases and 63.8% of the total amount of losses, making the crime the most prevalent (see Tables 5 and 6). Furthermore, with regard to "It's me" fraud, losses caused by a modus operandi in which a perpetrator poses as a police officer or similar authorities and defrauds cash or valuables under the pretext of an investigation (priority investigation) (known as fake police fraud) are prominent.

The number of recognized cases involving elderly victims (aged 65 and over) was 13,738, accounting for 65.4% of the total number of recognized cases excluding corporate losses.

Table 4: Trends in the Number of Recognized Cases and the Amount of Losses from Online and Telephone Fraud



	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
No. of recognized cases	13,392	13,824	14,154	18,212	17,844	16,851	13,550	14,498	17,570	19,038	21,043
Amount of damage	565.5	482.0	407.7	394.7	382.9	315.8	285.2	282.0	370.8	452.6	718.8

*1 General term for crimes that deceive an unspecified number of people out of cash and other assets by gaining their trust without face-to-face interaction, such as by making phone calls, and then getting them to transfer money to a designated deposit/savings accounts, among other methods. This includes crimes of extortion where cash is forcibly taken, as well as the fraudulent theft of cash cards.

*2 Investment fraud via social media: Fraud in which the offender deepens a relationship and gains the victim's trust through repeated communication via social media without meeting face to face, and then defrauds the victim of money under the pretense of investment funds or withdrawal fees for the profits (excluding cases falling under romance fraud via social media).
Romance fraud via social media: Fraud in which the offender deepens a relationship and gains the victim's trust through repeated communication via social media without meeting face to face, fosters romantic feelings and feelings of intimacy, and defrauds the victim of money.

Table 5: The Number of Recognized Cases by Modus Operandi

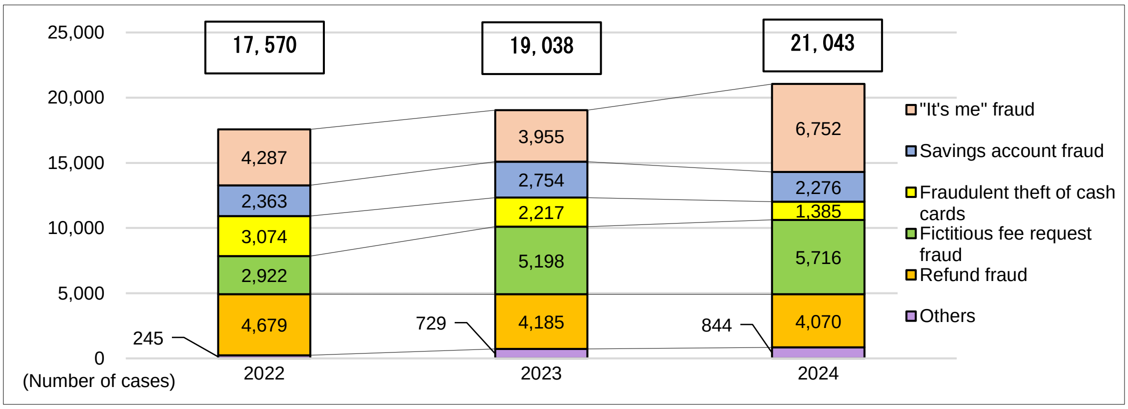
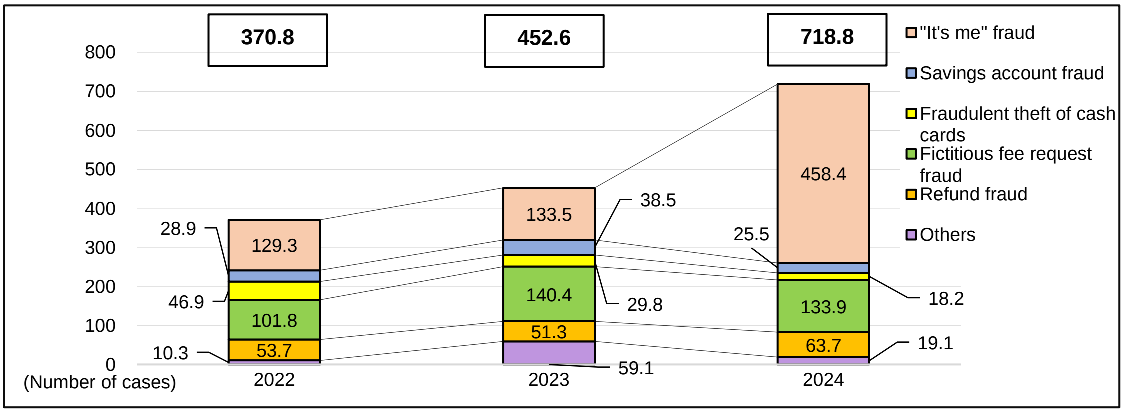


Table 6: The Amount of Losses by Modus Operandi



Note: As the figures are rounded to the nearest tenth, the total may not necessarily match the sum of the breakdown.

In 2024, the number of recognized cases of investment/romance fraud via social media was 10,237 cases, with total losses amounting to 127.19 billion yen. Both figures saw a significant increase compared to the previous year. The amount of losses was approximately 2.8 times higher than the previous year, while the number of recognized cases was approximately 2.7 times higher, making the situation extremely serious (see Table 7).

Looking at the number of recognized cases by prefecture, Osaka had the highest number of cases with 1,024, followed by Hyogo with 914, Tokyo with 877, Aichi with 675, Fukuoka with 664, Kanagawa with 538, and Hiroshima with 346. These seven prefectures accounted for 49.2% of the total number of recognized cases, indicating less concentration in major metropolitan areas compared to online and telephone fraud.

The average amount of losses per day was 347.52 million yen, and the average amount of losses per completed case was 12.427 million yen.

Table 7: Trends in the Number of Recognized Cases and the Amount of Losses from Investment/Romance Fraud Via Social Media

Charges	2023		2024	
	Number of Recognized cases	Amount of Losses (in 100 million yen)	Number of Recognized cases	Amount of Losses (in 100 million yen)
Investment Fraud Via Social Media	2,271	277.9	6,413	871.1
Romance Fraud Via Social Media	1,575	177.3	3,824	400.9
Total	3,846	455.2	10,237	1,271.9

(iii) Organized Theft and Trafficking of Stolen Goods

In recent years, organized metal theft[*1], vehicle theft, and large-scale shoplifting[*2] have been carried out by groups of illegal foreign residents and other criminals, with stolen goods being illegally exported overseas. These incidents have become a public safety issue.

The number of recognized cases of these thefts in 2024 include 7,054 cases of metal cable theft from solar power generation facilities (increased by 1,693 cases, or 31.6% compared to the previous year), 6,080 cases of vehicle theft (increased by 318 cases, or 5.5% compared to the previous year), and 981 cases of large-scale shoplifting from clothing stores and drugstores (decreased by 246 cases, or 20.0% compared to the previous year).

The number of cleared cases include 868 cases of metal cable theft from solar power generation facilities (increased by 552 cases, or 174.7% compared to the previous year), 2,683 cases of vehicle theft (increased by 221 cases, or 9.0% compared to the previous year), and 281 cases of large-scale shoplifting from clothing stores and drugstores (decreased by 24 cases, or 7.9% compared to the previous year).

Table 8: Status of Recognition and Clearance of Organized Theft and Trafficking of Stolen Goods

Metal cable theft from solar power generation facilities		Vehicle theft	
○2023 Number of Recognized Cases: 5,361 cases Number of Cleared Cases: 316 cases Rate of Cleared Cases: 5.9% Number of Offenders Arrested: 61 persons Number of Offenders Arrested (by Nationality) Cambodian: 36 persons Japanese: 24 persons Vietnamese: 1 person	○2024 Number of Recognized Cases: 7,054 cases Number of Cleared Cases: 868 cases Rate of Cleared Cases: 12.3% Number of Offenders Arrested: 147 persons Number of Offenders Arrested (by Nationality) Cambodian: 74 persons Japanese: 37 persons Thai: 19 persons Vietnamese: 8 persons Laotian: 5 persons Sri Lankan: 4 persons	○2023 Number of Recognized Cases: 5,762 cases Number of Cleared Cases: 2,462 cases Rate of Cleared Cases: 42.7% Number of Offenders Arrested: 745 persons Number of Offenders Arrested (by Nationality) Japanese: 682 persons Vietnamese: 18 persons Sri Lankan: 8 persons Brazilian: 8 persons Korean: 8 persons	○2024 Number of Recognized Cases: 6,080 cases Number of Cleared Cases: 2,683 cases Rate of Cleared Cases: 44.1% Number of Offenders Arrested: 600 persons Number of Offenders Arrested (by Nationality) Japanese: 516 persons Vietnamese: 24 persons Sri Lankan: 11 persons Pakistani: 10 persons Brazilian: 10 persons

Large-scale Shoplifting (Total losses amounting to 100,000 yen or more)			
Clothing Stores		Drugstores	
○2023 Number of Recognized Cases: 108 cases Number of Cleared Cases: 24 cases Rate of Cleared Cases: 22.2% Number of Offenders Arrested: 4 persons Number of Offenders Arrested (by Nationality) Vietnamese: 4 persons	○2024 Number of Recognized Cases: 79 cases Number of Cleared Cases: 65 cases Rate of Cleared Cases: 82.3% Number of Offenders Arrested: 12 persons Number of Offenders Arrested (by Nationality) Vietnamese: 10 persons Chinese: 1 person Mongolian: 1 person	○2023 Number of Recognized Cases: 1,119 cases Number of Cleared Cases: 281 cases Rate of Cleared Cases: 25.1% Number of Offenders Arrested: 133 persons Number of Offenders Arrested (by Nationality) Japanese: 65 persons Vietnamese: 47 persons Brazilian: 16 persons Chinese: 5 persons	○2024 Number of Recognized Cases: 902 cases Number of Cleared Cases: 216 cases Rate of Cleared Cases: 23.9% Number of Offenders Arrested: 91 persons Number of Offenders Arrested (by Nationality) Vietnamese: 50 persons Japanese: 40 persons American: 1 person

*Practical Statistics (March 2025, Criminal Affairs Bureau, National Police Agency)

[*1] Refers to theft in which the stolen goods are metal items (copper sheets, copper wire, drain covers, manholes, etc.).
[*2] Shoplifting with total losses amounting to 100,000 yen or more

*(iv) Illicit Commercial Practices Offences (Investment Fraud[*1] and Commercial Transaction Scam [*2])*

The number of cleared cases of Fraudulent Investment Solicitation in 2024 was 49, an increase of 6 cases (14.0%) from the previous year. The number of offenders arrested was 162, an increase of 35 offenders (27.6%) from the previous year.

Looking at the number of cleared cases by type, 21 cases (42.9% of the total) were offences related to deposits, including offences under the pretext of investments in international financial transactions such as FX or cryptoassets-related businesses. The amount of losses in 2024 amounted to approximately 177.6 billion yen (see Table 9).

The number of cleared cases of commercial transaction scam in 2024 was 113, an increase of 5 cases (4.6%) from the previous year. The number of offenders arrested was 228, an increase of 34 offenders (17.5%) from the previous year.

Looking at the number of cleared cases by type, 92 cases (81.4% of the total) were offences related to door-to-door sales, including offences related to home remodeling contract such as roof repair work. The amount of losses in 2024 amounted to approximately 9.8 billion yen (see Table 10).

Table 9: Trends in the Amount of Losses from Investment Fraud

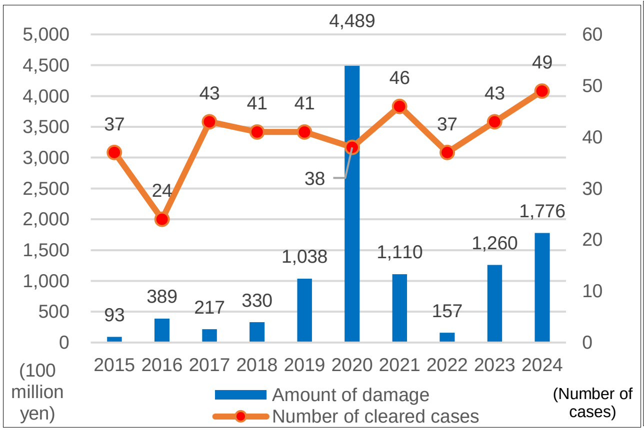
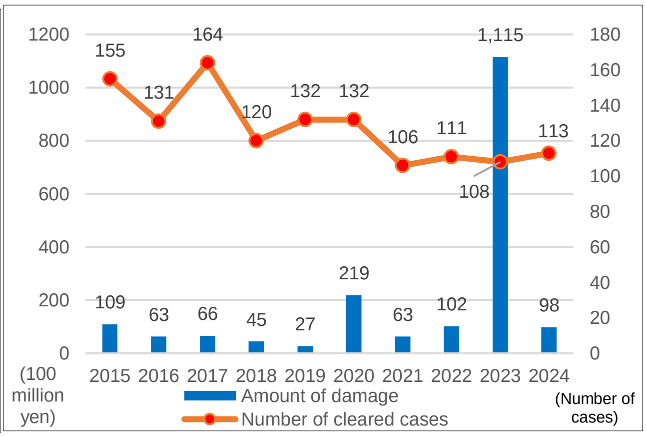


Table 10: Trends in the Amount of Losses from Commercial Transaction Scam



*(v) Cyber Crimes[*3]*

The following situations were observed regarding the threat to the situation surrounding cyberspace[*4] in 2024:

○ Threat Situation of Cyber Attacks Involving the Misuse of Advanced Technologies

During 2024, cyber attacks aimed at information theft and cyber attacks backed by nation-states aimed at acquisition of cryptoassets occurred in succession. In addition, from the end of the year to the beginning of the following year, incidents resembling DDoS attacks were reported against financial institutions and other entities. Furthermore, the number of reported ransomware incidents remained at a persistently high level.

○ Threat Situation of Crimes Involving the Misuse of Cyberspace

---

[*1] Offences related to violations of the Investment Act (prohibition of deposits, etc.), the Financial Instruments and Exchange Act (Act No. 25 of 1948), Act on Prevention of Pyramid Schemes (Act No. 101 of 1978), the Act on Deposit Transactions (Act No. 62 of 1985) (including cases that, as a result of investigation, are found to constitute fraud)

[*2] Offences related to violations of the Act on Specified Commercial Transactions (Act No. 57 of 1975) and fraud, extortion, etc., concerning commercial transaction scam.

[*3] Incidents that harm cybersecurity or involve the misuse of information technology, potentially endangering the life, body, and property of individuals as well as public safety and order.

[*4] For details, refer to "Threat Situation surrounding Cyberspace in 2024" (March 2025, Cyber Affairs Bureau, National Police Agency).

Not only in online banking fraud cases, but also in investment/romance fraud via social media, cryptoassets are being used for ML, demonstrating the misuse of online services.

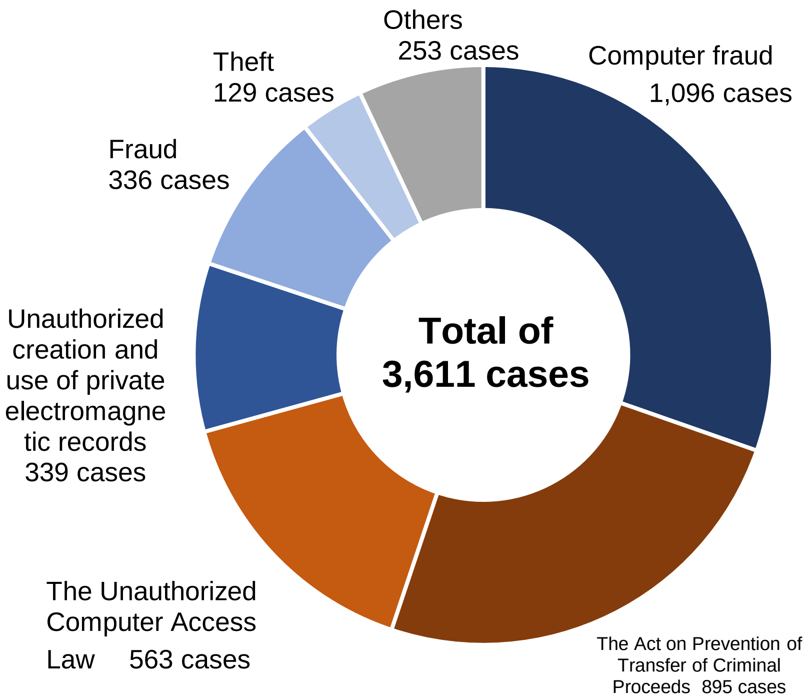
○ Situation Regarding Illegal and Harmful Information

Social media platforms are flooded with recruitment messages for criminal actors using phrases like “white jobs.” Furthermore, during the 2024 Noto Peninsula Earthquake, images from past disasters and false rescue information were widely disseminated.

○ Clearance of Cyber Crimes

In the clearance of cyber crimes in 2024, violations of the Act on Prevention of Transfer of Criminal Proceeds ranked second only to computer fraud. Violations of the Act on Prevention of Transfer of Criminal Proceeds that fall under cyber crimes involve providing user IDs, passwords, and similar credentials for online banking and other services using highly anonymous communication methods via the internet.

Table 11: Breakdown of Clearance of Cyber Crimes in 2024



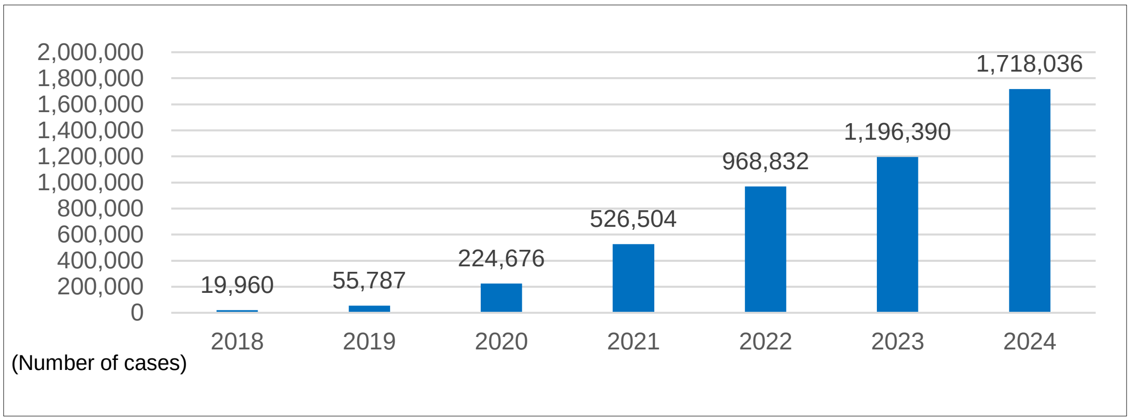
(A) Situation of Phishing[*1]

The number of reported phishing cases in 2024 was 1,718,036, continuing its upward trend[*2]. Information fraudulently obtained through phishing is being misused for unauthorized fund transfers related to online banking and fraudulent credit card use, among other purposes.

[*1] A modus operandi where emails or SMS messages are sent pretending to be from real companies, organizations, or government agencies, directing recipients to view a fake website (phishing site) designed to look like the company’s website, and then illegally obtaining account information, credit card numbers, etc., from that phishing site.

[*2] Based on a survey by the Council of Anti-Phishing Japan.

Table 12: Trends in the Number of Reports in Phishing

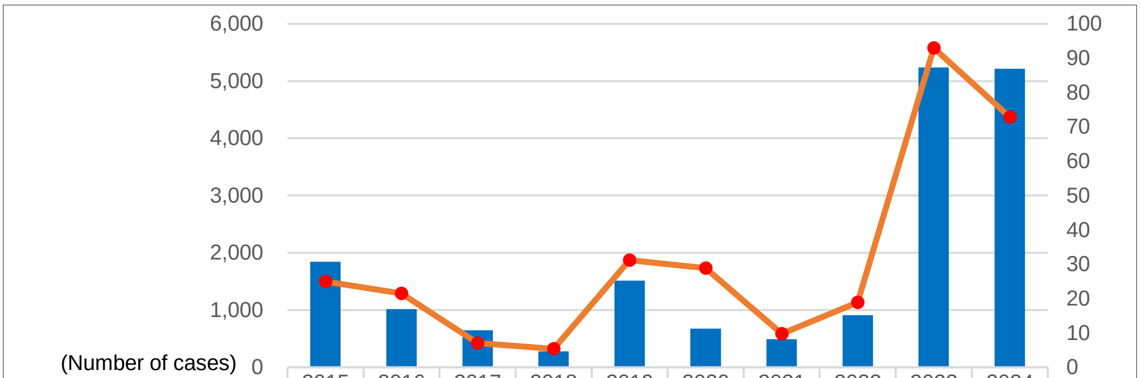


(B) Situation of Online Banking Fraud Cases

In 2024, the number of online banking fraud cases was 4,369, and the amount of losses was approximately 8.69 billion yen. Approximately 90% of these incidents are believed to have been perpetrated through phishing. The following characteristics were observed in the online banking fraud cases in 2024:

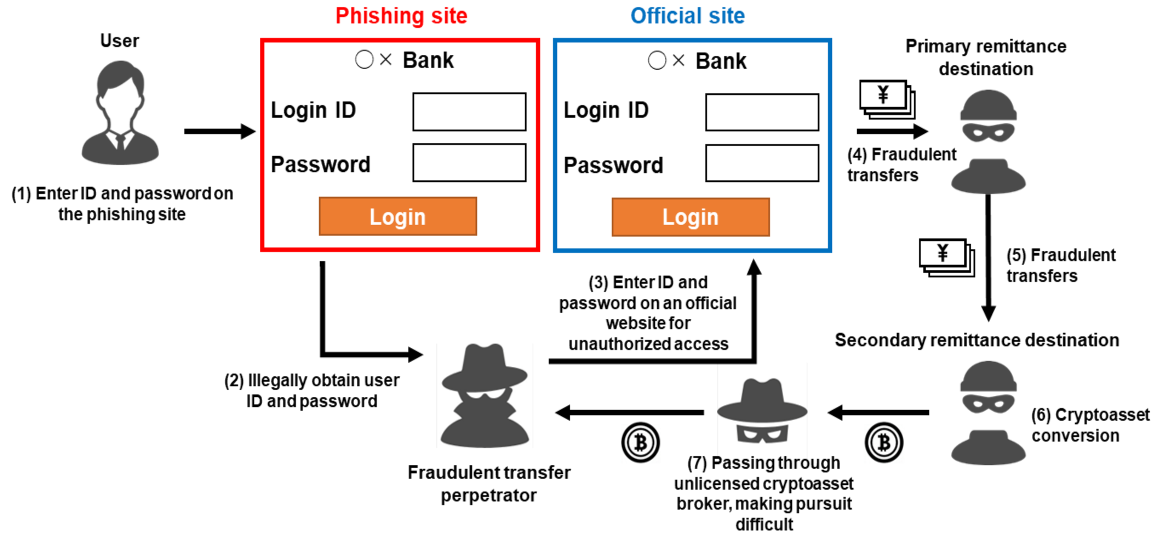
- Fraudulent fund transfers from corporate accounts via voice phishing (phishing using voice calls) are rapidly increasing
- Other modus operandi besides phishing include cases triggered by malware infection and SIM swapping to bypass identity verification
- Of the total losses, 3.21 billion yen was used to transfer funds to cryptoassets exchange service providers

Table 13: Trends in the Number of Online Banking Fraud Cases



	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Amount of damage	30.7	16.9	10.8	4.6	25.2	11.3	8.2	15.2	87.3	86.9
Number of cases	1,495	1,291	425	322	1,872	1,734	584	1,136	5,578	4,369

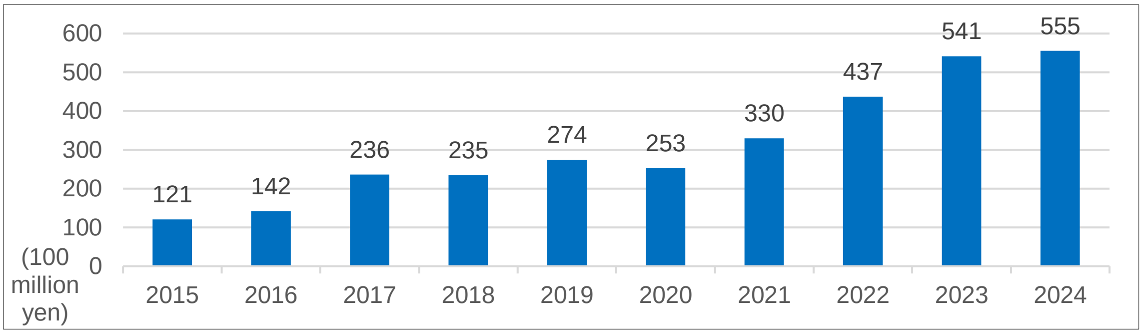
Table 14: Flow of Online Banking Fraud



(C) Situation of Credit Card Fraud

The amount of losses caused by credit card fraud in 2024 amounted to approximately 55.5 billion yen, marking the highest amount on record[*1]. Among these credit card fraud cases, some involved converting criminal proceeds into cryptoassets for ML purposes.

Table 15: Status of Credit Card Fraud Losses



(D) Situation of Ransomware

In 2024, the number of ransomware attack cases reported to the National Police Agency was 222, still remaining at a high level. In addition to losses caused by ransomware, 22 cases[*2] of losses from “no-ware ransom,” that is, encryption-less ransomware, where offenders intrude company or organization network, steal data without encrypting it and then demand payment, have been confirmed.

Characteristics of ransomware in recent years include:

● A significant number incidents involve double extortion[*3]

● The involvement of multiple actors dividing roles to orchestrate attacks, reducing the need for crime actors to possess advanced technical knowledge and thereby broadening the pool of attackers

---

[*1] According to a survey by the Japan Consumer Credit Association.

[*2] The number of cases of “no-ware ransom” is not included in the number of reports on ransomware losses in 2024 (222 cases).

[*3] “Double-extortion” means that criminals demand a ransom (in money or cryptoassets) from companies and organizations after encrypting and stealing data from them by saying “the data will be disclosed if payment is not made.”

When comparing the number of reports on ransomware losses by organizational size to 2023, the number of reports on losses among large enterprises has decreased, while the number of reports on losses among small and medium-sized enterprises has increased. This suggests that the broadening base of attacking crime actors is leading to increased losses among small and medium-sized enterprises, where countermeasures are comparatively weaker.

Table 16: Flow of Ransomware Attacks

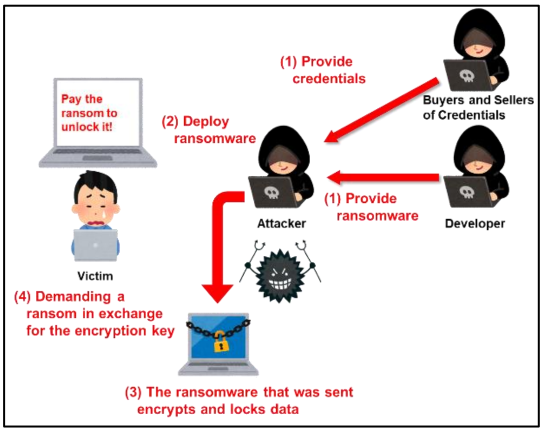
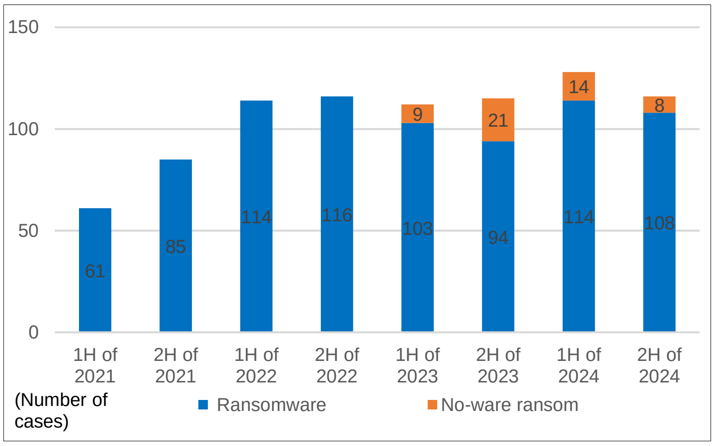


Table 17: Trends in the Number of Reports on Ransomware Losses



(E) Cyber Attacks Suspected to be State-Sponsored

In 2024, cyber attacks suspected to be state-sponsored were confirmed with the aim of stealing cryptoassets and other digital assets and acquiring foreign currency. In May of the same year, a cyber-attack group backed by North Korea, Trader Traitor, stole cryptoassets worth approximately 48.2 billion yen from a domestic cryptoassets exchange service provider[*1].

(vi) Gold smuggling

In the 2023 administrative year*[2], the number of processed cases of gold smuggling (accusations filed with prosecutors or notifications issued by customs directors) was 102, representing an 18% decrease compared to the previous administrative year. On the other hand, the value of evaded taxes was about 360 million yen, an increase of approximately 2.1 times compared to the previous administrative year.

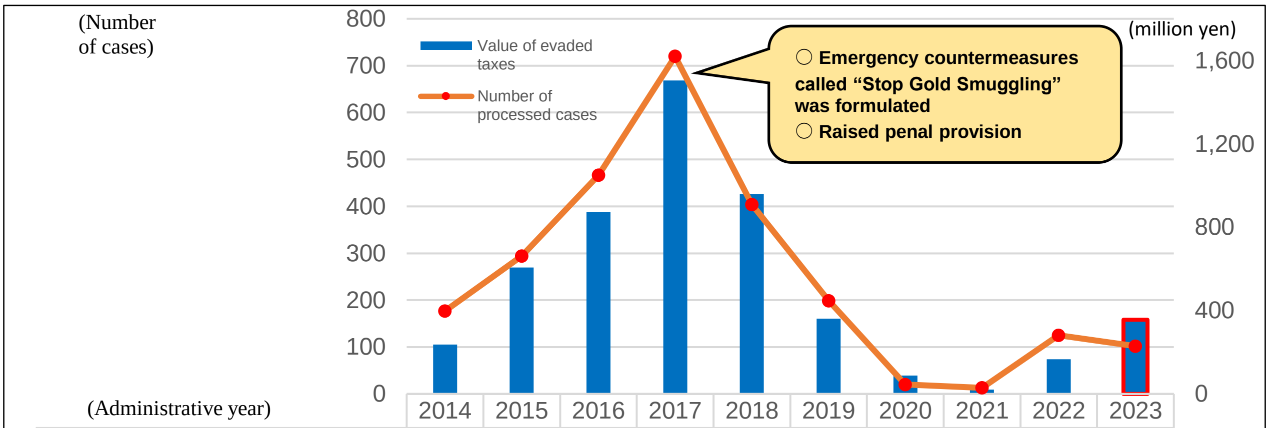
Since the penal provision against gold smuggling were raised substantially in 2018[*3], both the number of cases of gold smuggling and the amount of tax evaded had been decreasing. However, gold smuggling is on the rise again in the 2022 administrative year due to factors such as the rising price of gold and the termination of border control measures implemented as COVID-19 countermeasures, coupled with a sharp increase in the number of foreign visitors to Japan. Furthermore, the amount of tax evaded increased substantially in the 2023 administrative year, so future trends should be closely monitored.

[*1] Regarding the occurrence of this incident, in December 2024, the National Police Agency, in cooperation with the United States, identified it as a theft case perpetrated by "Trader Traitor." Furthermore, in January 2025, the governments of Japan, the United States, and the Republic of Korea issued a joint statement concerning on North Korea's cryptoassets theft and public-private collaboration.

[*2] The period from July 2023 to June 2024.

[*3] The Act for Partial Revision of the Customs Tariff Act (Act No. 8 of 2018)

Table 18: The Number of Processed Cases of Gold Smuggling and the Value of Evaded Taxes



	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Value of evaded taxes	237	607	874	1,504	960	361	89	20	167	356
Number of processed cases	177	294	467	720	404	199	20	13	125	102

(vii) Online Casinos

It has been pointed out that the number of Japanese people accessing overseas online casino sites from within Japan has increased in recent years, suggesting that a growing number of Japanese gamblers have been accessing online casino sites from PCs in their homes, illegal gambling establishments, and elsewhere. Online gambling offenses have actually resulted in arrests.

Table 19: Status of Cleared Cases of Online Gambling Offences[*1]

Category \ Year	2021	2022	2023	2024
Number of cleared cases	16	10	13	62
Number of offenders arrested	127	59	107	279

[*1] In addition to cases where gamblers access online casino sites directly via computers at home or elsewhere to engage in gambling, cases where gamblers use personal computers installed at gambling establishments or similar venues to play games distributed by online casino site operators are counted as online gambling offences.

***[Topic] The Actual Situation and Characteristics of Online Casinos** [*1]*

1. Research Study to Understand the Actual State of Online Casinos

While online casinos are legally operated in certain countries and regions, accessing them from within Japan to engage in gambling constitutes a crime, even if the operator is legal in its country or region of origin. In recent years, an increase in the number of accesses to online casino sites operated overseas has been noted, and there have been cases where domestic gamblers and entities referring to themselves as payment or collection agents[*2] have been arrested. The National Police Agency has commissioned a private contractor to ascertain the actual usage of online casinos and gather information on the sites. In March 2025, the "Outsourced Research Report on Research Study to Understand the Actual State of Online Casinos" (hereinafter referred to as the "Research Report") was published.

The main contents of the Research Report are as follows.

(1) Market Size Estimate

The estimated number of domestic online casino users aged 15 to 79 is approximately 1.967 million, with total annual wagers projected at around 1.2423 trillion yen. By age group, those in their 20s show the highest usage rate (5.8%). Furthermore, the highest total wagers are recorded among those in their 30s, at approximately 460.6 billion yen. This indicates that the younger demographics of those in their 20s and 30s constitute the majority of the market size.

Table 20: Market Size Estimate for online casinos by Age Group[*3]

Age Group	Total population (thousand people)	Online Casino Usage Rate (%)	User Population (people)	Wagers/year (yen)	Total wagers/year (yen)
Total	97,575	2.02	1,967,133	631,523	1,242,289,566,650
10s	5,494	1.63	89,501	303,833	27,193,464,077
20s	12,715	5.80	738,024	620,120	457,663,724,985
30s	13,427	4.29	575,641	800,229	460,644,727,649
40s	16,880	2.10	353,984	576,563	204,094,143,200
50s	17,929	0.66	118,032	580,692	68,540,042,032
60s	14,839	0.40	58,899	229,950	13,543,748,973
70s	16,291	0.20	33,052	321,000	10,609,715,735

(2) Online Casino Sites Confirmed to Be Used from within Japan

When asked which online casino sites they had used, the most frequently used site among online casino users was "Vera & John," with 37.2% reporting experience using this casino. This is followed by "Casino Secret" at 25.0%, "Queen Casino" at 21.2%, and "Yuugado" at 20.2%.

All of the online casino sites surveyed[*4] were found to be operated under licenses obtained abroad. Licenses from Curacao (Netherlands) were particularly prominent, accounting for the majority of the 40 sites. Licenses from other countries and regions were also confirmed, including Anjouan (Comoros), Costa Rica, Malta, Gibraltar (UK), the Isle of Man (UK), and Georgia.

---

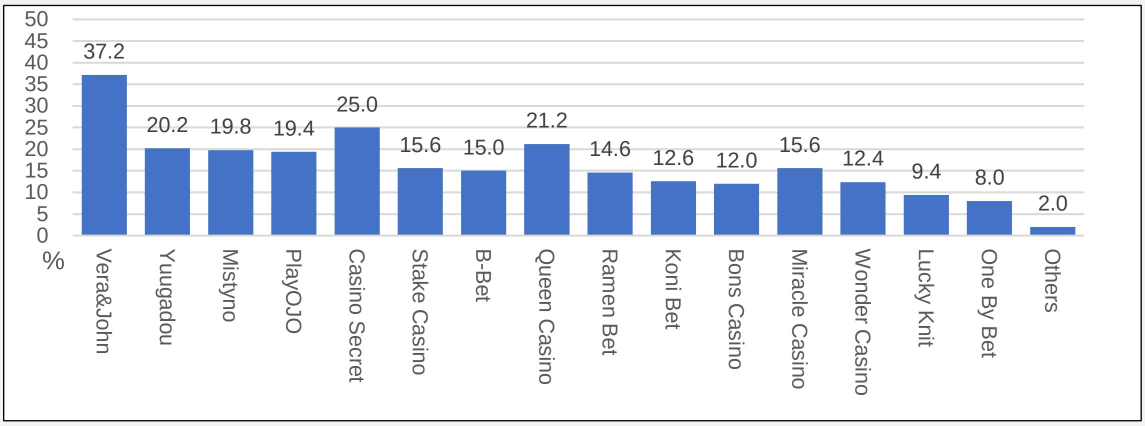
*1 The 2024 NRA-FUR, "Topic: Report on Money Laundering and International Organized Crime Related to Online Casinos," also introduces the characteristics and typologies of ML using online casinos.

*2 Regarding business models referred to as "payment agent" or "collection agent," there currently exists no unified definition for the business type itself, nor any statutory registration or licensing system. Consequently, the actual business activities conducted by operators using these names are not uniform.

*3 Quoted from Table 6 on page 8 of the research report

*4 The survey was limited to sites that can be searched from general platforms, and identified top 40 frequently featured sites from seven comparison sites introducing online casinos for Japanese players, which were selected as the subjects of this survey.

Table 21: Online casino sites respondents indicated they have used[*1]

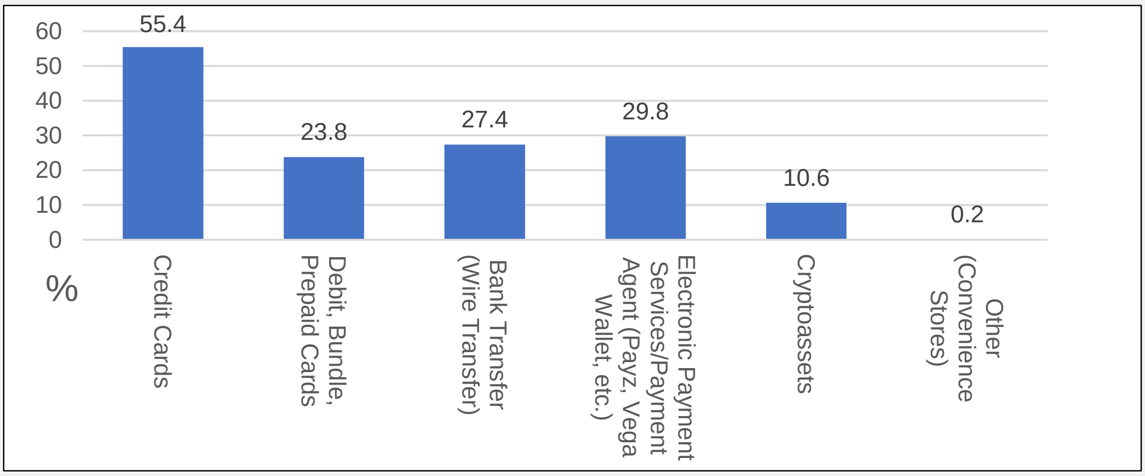


(3) Deposit Methods for Online Casinos

Various options exist for depositing funds into online casinos. Primary deposit methods include credit cards and e-wallets[*2] (e.g., Vega Wallet, Payz, Jeton Wallet). These methods are characterized by instant deposit processing. Cryptoassets (e.g., Bitcoin, Ethereum) are also widely accepted, offering advantages such as anonymity and immediacy. Furthermore, most online casinos also support bank transfers.

A survey of experienced online casino users regarding deposit methods yielded the results shown in Table 22.

Table 22: Deposit Methods for Online Casinos[*3]



2. Initiatives by Competent Authorities

In May 2025, the Financial Services Agency and the National Police Agency requested that industry associations for deposit-taking institutions, the Japan Payment Service Association, and the Japan Virtual and Cryptoassets Exchange Association inform their member financial institutions of the following three points regarding measures to prevent gambling offences related to online casinos:

- Warn users that accessing online casino sites and gambling within Japan constitutes a crime.
- Clearly state in the terms of service for such services that the use of payment services for illegal activities, including gambling offences at online casinos, or acts contrary to public order and morals is prohibited.
- Suspend any payment transaction when it is determined that the user is attempting to make a payment on an online casino site, whether domestic or international.

[*1] Quoted from Table 34 on page 35 of the research report (multiple answer questions)

[*2] This appears to be an electronic payment service where users exchange virtual points or balances, but it does not refer to prepaid payment instruments or funds transfer services under Japan's Payment Services Act.

[*3] Quoted from Table 38 on page 39 of the research report (multiple answer questions)

3. Measures by Specified Business Operators

Examples of risk mitigation measures taken by specified business operators include:

- Sending emails to all customers warning them that “using online casinos constitutes a crime”
- Conducting direct interviews and warnings for customers suspected of using online casinos through transaction monitoring
- Implementing warnings via the transaction app for customers suspected of using online casinos through monitoring of access information, etc.
- When reviewing account opening applications for corporations suspected of providing payment and collection services, verifying the actual business operations via the Internet and conducting additional interviews regarding products and counterparties, etc., before deciding whether to allow account opening. Furthermore, refusing to allow account opening if it is determined that the entity is related to online casinos

4. Flow of Funds Related to Online Casinos

Regarding online casinos, as shown in Table 23, funds flow from gamblers to online casino site operators through accounts held by entities claiming to be payment and collection agencies. A revenue structure is also observed where affiliate marketers receive rewards for advertising and promoting online casinos.

Furthermore, as shown in Table 24, regarding the flow of funds through accounts of entities claiming to be payment or collection agents, there are also cases where funds pass through multiple corporatenamed accounts and are ultimately transferred to accounts located overseas.

Table 23: Examples of Revenue Structures Related to Online Casinos

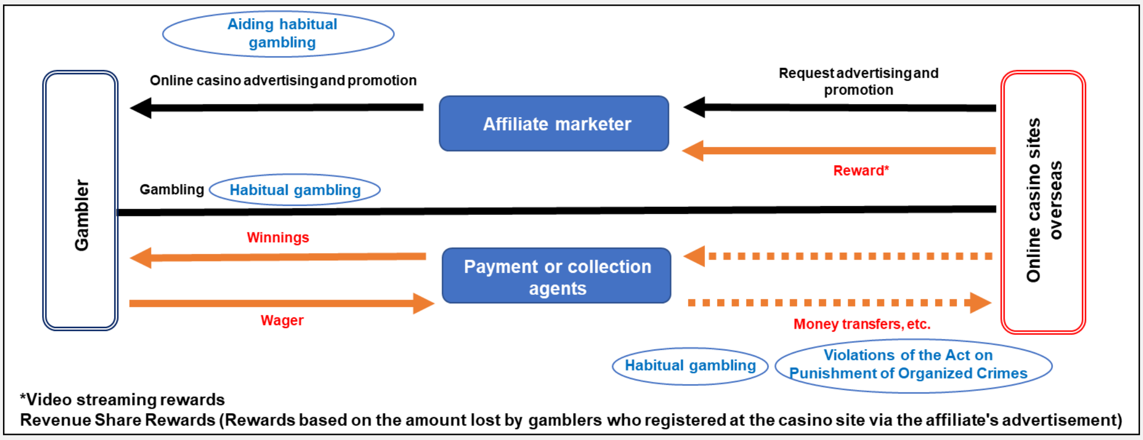
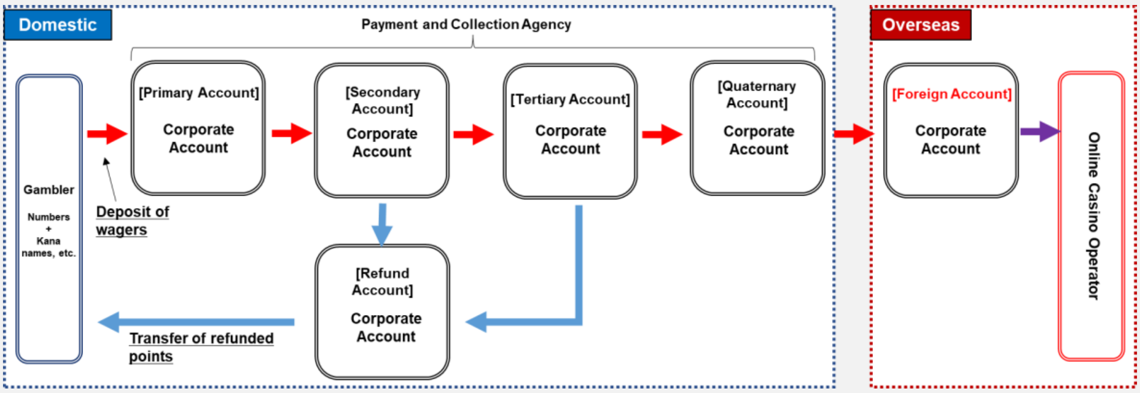


Table 24: Illustration of Flow of Funds Related to Online Casinos



[Comprehensive Measures to Protect People from Frauds 2.0*1]

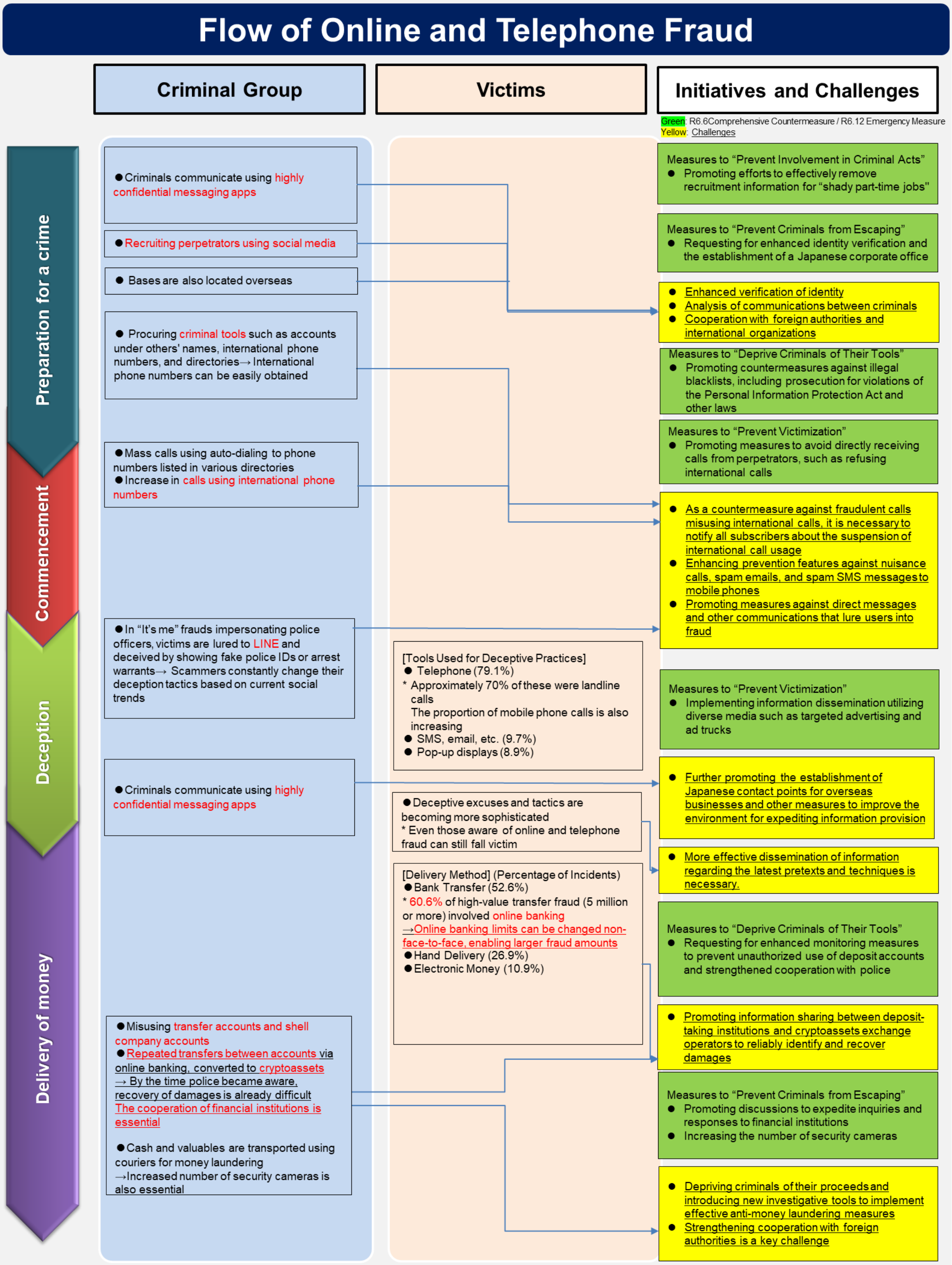
Amid the spread of social media and cashless payments, and the accelerating growth of fraud and other crimes misusing these technologies, the "Comprehensive Measures to Protect People from Frauds" (adopted at the Ministerial Conference on Measures against Crime on June 18, 2024; hereinafter referred to as the "Comprehensive Fraud Countermeasures") was developed, and measures were taken in cooperation with the public and private sectors. However, the amount of losses from offences against property in 2024 exceeded 400 billion yen. Of this amount, the amount of losses from frauds amounted to approximately 307.5 billion yen, making further measures against fraud an urgent necessity.

In order to protect people from increasingly complex and sophisticated fraud and other crimes, it was deemed necessary not only to swiftly update countermeasures in response to evolving modus operandi, but also to undertake efforts such as uncovering the true nature of criminal groups to apprehend them and sever the points of contact between criminal groups and victims. Therefore, in April 2025, the "Comprehensive Measures to Protect People from Frauds 2.0" (adopted at the Ministerial Conference on Measures against Crime on April 22, 2025; hereinafter referred to as "Comprehensive Fraud Countermeasures 2.0"), revised the previous Comprehensive Fraud Countermeasures. This initiative fundamentally strengthens the government's overall efforts against fraud and similar crimes.

The Comprehensive Fraud Countermeasures 2.0 integrates the existing Comprehensive Fraud Countermeasures with the "Emergency Measures to Protect People's' Lives and Property from Robberyand Other Crimes Committed Through "Shady Part-time Jobs" (adopted at the Ministerial Conference on Measures against Crime on December 17, 2024), and amends the existing Comprehensive Fraud Countermeasures by adding new initiatives such as measures to prevent the misuse of financial and communications services and infrastructure, and the consideration of new investigative methods using fictitious accounts. In developing the Comprehensive Fraud Countermeasures 2.0, measures and issues were examined at each stage of the points of contact between criminal groups and victims for each category of fraud and other crimes, and online and telephone fraud were organized as shown in Table 25.

*1 For more details, please refer to the Prime Minister's Office website (https://www.kantei.go.jp/jp/singi/hanzai/index.html)

Table 25: Flow of Online and Telephone Fraud[*1]



[*1] Excerpt from Materials for the 42nd Meeting of the Ministerial Conference on Measures against Crime held on April 22, 2025

(2) Terrorism Situation

As for the international terrorism situation, ISIL*1 continues to call on sympathizers to carry out attacks against Western and other countries participating in the Global Coalition to Counter ISIL. Furthermore, AQ*2 and its related organizations operating in the Middle East and Africa continue to carry out terrorist attacks targeting local government agencies. In December 2024, anti-government forces led by HTS*3 overthrew the Assad regime in Syria, establishing a provisional government with HTS's leader as president. However, the situation remains unstable, and it has been pointed out that international terrorist organizations, including ISIL, may attempt to exploit this situation to carry out terrorist attacks.

In addition, following the terror attacks on Israel by Hamas and other Palestinian militants in October 2023 and the subsequent armed conflict, ISIL, AQ and their affiliates and supporters have been calling for attacks against Israel and Western interests, and terrorist incidents believed to be related to this situation have occurred in various countries.

In addition to these incidents, terrorist incidents are occurring around the world, and given that there have been actual cases in the past where Japanese nationals and Japan's national interests were targeted by terrorist attacks, there are ongoing concerns that Japanese nationals may continue to fall victim to terrorist attacks and kidnappings.It can be therefore said that the threat of terrorism against our country persists. Although many years have passed since suspected abduction cases by North Korea, not all victims have yet returned to Japan. Time is running out to resolve this issue.

In addition to these situations, government agencies and companies are being targeted globally by attacks in cyberspace. Japan faces the threat of cyber terrorism that will paralyze the society's functions.

---

*1 The acronym for the Islamic State in Iraq and the Levant. Commonly known as the Islamic State.
*2 Abbreviation for Al-Qaeda.
*3 Abbreviation for Hayat Tahrir al Sham

Section 3. Analysis of Money Laundering Cases

This section analyzes the "offenders" and "predicate offences" that generate criminal proceeds, constituting the threat of ML/TF in Japan, from the perspective of cleared ML cases.

It will also analyze the "major transactions misused for ML/TF", where vulnerability to ML/TF is recognized.

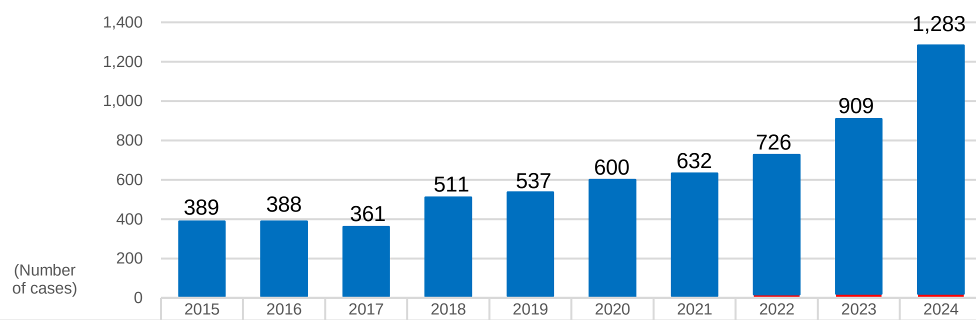
The overview is as follows:

Threat	Offenders	Anonymous and fluid criminal groups, Boryokudan, Crime groups of foreigners in Japan	
	Predicate Offences	Major Predicate Offences	Fraud, Computer fraud, Theft, Violation of the Investment Act/Money Lending Business Act, Habitual gambling/running a gambling venue for profit, Violation of the Immigration Control and Refugee Recognition Act, Violation of the Amusement Business Act/Violation of the Anti-Prostitution Act, Trafficking in person offences, Investment Fraud offences, Drug-related offences
Vulnerability factor	Major transactions misused for ML/TF		Domestic exchange transactions, Cash transactions, Credit card, Prepaid payment instruments, Deposit transactions, Cryptoassets, Legal persons, Funds transfer services, Cross-border transaction, Financial instruments, Precious metals and stones, Electronic payment instruments, Real estate, Money lending, Foreign currency exchanges, Legal/Accounting professionals, Bills and checks, Postal receiving services

Regarding the Suspicious Transaction Report (STR), it also describes the reporting status of STRs by business type, the usage status of STRs in criminal investigations, and investigations of non-criminal offence cases.

The number of cleared ML cases[*1] in 2024 was 1,283, an increase of 374 cases compared to the previous year (see Table 26). In recent years, there has been a notable increase in the number of cleared cases for violations of the Act on Punishment of Organized Crimes among ML offences. Factors contributing to this include the establishment of investigative techniques for ML offences, as well as an increase in the occurrence of predicate offences such as online and telephone fraud and investment/romance fraud via social media. Consequently, there has also been a rise in cases where criminal proceeds obtained through these predicate offences are subsequently laundered.

Table 26: The Number of Cleared ML Cases



	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Violations of the Act on Punishment of Organized Crimes	381	380	353	504	528	597	623	709	888	1,262
Violations of the Anti-Drug Special Provisions Act	8	8	8	7	9	3	9	17	21	21

*1 The offences set forth in Articles 9, 10 and 11 of the Act on Punishment of Organized Crime as well as Articles 6 and 7 of the Anti-Drug Special Provisions Act.

In addition, it is important to confiscate criminal proceeds in order to prevent them from being used to maintain and expand criminal organizations or to invest in future criminal activities. In this regard, the following Table shows the status of issuance of preservation order for confiscation before prosecution as well as the application of the confiscation and collection provisions of the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act in ordinary trial proceedings at the court of first instance from 2022 to 2024.

Table 27: Status of Confiscation of Criminal Proceeds

			2022	2023	2024
Preservation for confiscation before prosecution					
	Act on Punishment of Organized Crimes	Number of cases	162	211	225
		Total amount of money and claims (thousand yen)	1,047,244	1,044,378	1,964,173
	Anti-Drug Special Provisions Act	Number of cases	23	20	27
		Total amount of money and claims (thousand yen)	25,363	45,427	23,905
Confiscation					
	Act on Punishment of Organized Crimes	Number of persons	76	119	110
		Total amount of money and claims (thousand yen)	205,665	353,107	491,081
	Anti-Drug Special Provisions Act	Number of persons	56	54	50
		Total amount of money and claims (thousand yen)	5,678	8,404	6,767
Collection of a sum of equivalent value					
	Act on Punishment of Organized Crimes	Number of persons	92	103	99
		Total amount of money and claims (thousand yen)	1,342,766	1,267,096	1,764,624
	Anti-Drug Special Provisions Act	Number of persons	223	199	166
		Total amount of money and claims (thousand yen)	860,989	394,534	474,201

Note: 1. Preservation orders for confiscation before prosecution are limited to those requested by judicial police officers.
2. Information on confiscation and collection of a sum of equivalent value is based on Ministry of Justice data as of the end of March 2025.
3. Amounts are rounded down to the nearest thousand yen.
4. For confiscation and collection of a sum of equivalent value issued to accomplices in duplicate, the amount is recorded after deducting the duplicate amount.
5. The confiscated and collected foreign currency was converted to Japanese yen at the exchange rate as of the date of judgment.

1. Offenders

In general, money laundering refers to an act of concealing the sources or real owners of criminal proceeds in an attempt to prevent investigating authorities from discovering the proceeds or clearing the case. Criminals who illegally acquire property may commit ML, and there are various types of ML offenders, regardless of their nationality, type of crime, or whether or not they are organized. In Japan, the main types of offenders engaged in organized ML are “Anonymous and fluid criminal groups,” “Boryokudan,” and “Crime groups of foreigners in Japan.”

Note that this article analyzes Anonymous and fluid criminal groups and Crime groups of foreigners in Japan as separate types of offenders, but some Crime groups of foreigners in Japan are also included in Anonymous and fluid criminal groups.

(1) Anonymous and fluid criminal groups

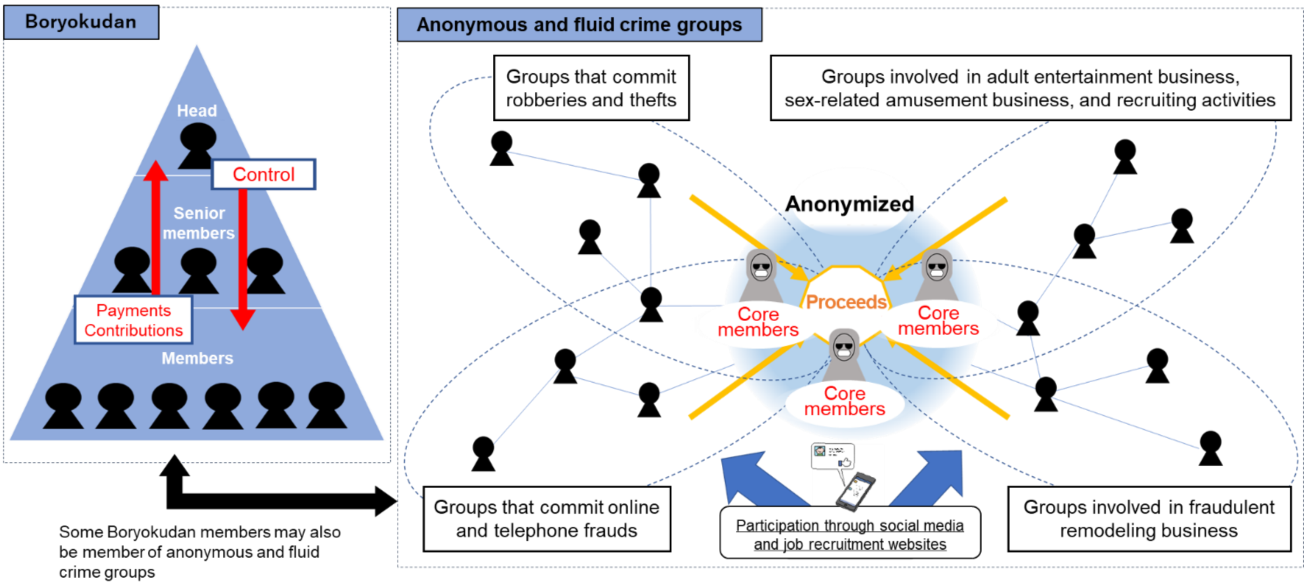
(i) Characteristics

In recent years, as the power of Boryokudan has been declining, “Anonymous and fluid criminal groups” with new characteristics have emerged in addition to quasi-Boryokudan that are mainly composed of former members of Boryokudan and former members of motorcycle gangs and are operating in bustling areas and nightlife spots, posing a threat to public security measures. Boryokudan is bound by fictitious blood ties among their members and is often hierarchically structured under the control of a “Kumicho (boss),” with members ranked according to status. They conducted fund-raising activities backed by or exploiting the power of the organization. In contrast, Anonymous and fluid criminal groups operate in a manner whereby the core members who consolidate and siphon off proceeds from revenue-generating activities remain anonymised. Furthermore, members loosely connected through social media or job recruitment sites subdivide roles and, on a case-by-case basis, recruit individuals who respond to postings related to criminal activities as “disposable” low-level perpetrators. By constantly rotating members while conducting diverse revenue-generating activities, they make it difficult to identify their organizational structure or specific members.

Anonymous and fluid criminal groups commit a variety of crimes, including online and telephone fraud, organized robbery and theft, illegal scouting, fraudulent remodeling business, and drug trafficking, and use the proceeds as a major source of funding. Furthermore, a structure is observed in which the core members of the organization make profits while recirculating the proceeds, such as by using funds acquired through crime for new revenue-generating activities such as adult entertainment.

Furthermore, it has also been confirmed that some of such funds appear to be flowing to Boryokudan, that there are groups that have Boryokudan gangsters as leaders or members, and that there are groups that conspire with Boryokudan gangsters to commit crimes. As such, while there are some relationships between Boryokudan and Anonymous and fluid criminal groups, it appears that there are also individuals who act as hubs between the two.

Table 28: Characteristics of Boryokudan and Anonymous and fluid criminal Groups



(ii) Revenue-Generating Crimes

Regarding the revenue-generating crimes[*1] believed to be committed by Anonymous and fluid criminal groups in 2024, looking at the 5,203 people arrested for the main revenue-generating crimes[*2] by type of crime, there were 2,655 fraud cases, which accounted for the largest number, followed by 991 theft cases, 917 drug-related offences, 348 robbery cases, and 292 violation of the Amusement Business Act. It suggests that Anonymous and fluid criminal groups are involved in wide range of cases and are engaged in a variety of revenue-generating activities, including online and telephone fraud and investment/romance fraud via social media, as well as organized robbery[*3], malicious host club offences, organized theft and distribution of stolen goods, malicious home remodeling offences, and cyber crimes[*4] such as online banking fraud cases.

(A) Organized Robbery

Among the organized robberies and other offences attributed to Anonymous and fluid criminal groups, there have been cases where perpetrators were recruited on social media and job recruitment sites using phrases such as “high-paying part-time job,” “so-called ‘white’ job offers” and “same-day payment.” Some of these robberies and other offences have involved particularly violent methods, including restraining and assaulting victims. These robberies and other offences, occurring frequently in the Kanto region since August 2024, have significantly worsened the public sense of security.

(B) Online and Telephone Fraud

The forms of payment for these online and telephone fraud include direct face-to-face methods like cash handover, cash card handover, and cash card theft as well as non-face to-face methods like bank transfer, cash mailing, electronic money and other means. Regarding the recognized cases by form of payment, the number of recognized cases of bank transfer type increased by 4,564 compared to the previous year to 11,060, accounting for 52.6% of the total number of recognized cases and 58.6% of the total amount of losses (see Tables 29 and 30).

Regarding the use of online banking for transfer type with the amount of losses exceeding 5 million yen (the number of recognized cases of 1,673, the amount of losses of 30.77 billion yen), the number of recognized cases was 1,020, with the amount of losses of 21.03 billion yen. This represents 61.0% of recognized cases and 68.3% of the amount of losses within all transfer type with the amount of losses exceeding 5 million yen.

[*1] Revenue-generating crimes committed by Anonymous and fluid criminal groups refer to crimes that may lead to the procurement of funds for the activities of Anonymous and fluid criminal groups, and include online and telephone fraud, robbery, illicit trafficking of stimulants, the collection of protection money from restaurants and other businesses in entertainment districts, extortion or compulsion targeting companies and administrative agencies, theft, and fraud that abuses public subsidy systems, as well as illegal money lending businesses, adult entertainment store management, and labor supply businesses such as scouting for adult videos, all disguised as ordinary economic transactions.

[*2] Fraud, robbery, theft, drug-related offences, and violation of the Amusement Business Act.

[*3] Robbery, theft, trespassing into a residence and a building, etc.

[*4] Violations of the Unauthorized Computer Access Law, offences involving computers or electromagnetic records, and other offences utilizing advanced information and telecommunication networks as an indispensable means for their execution

Table 29: Number of Recognized Cases by Form of payment

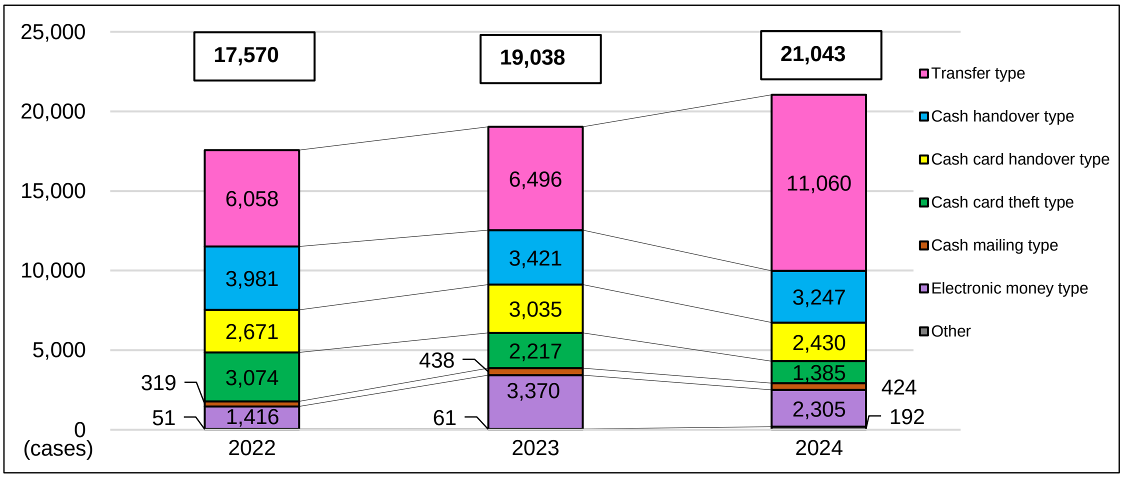
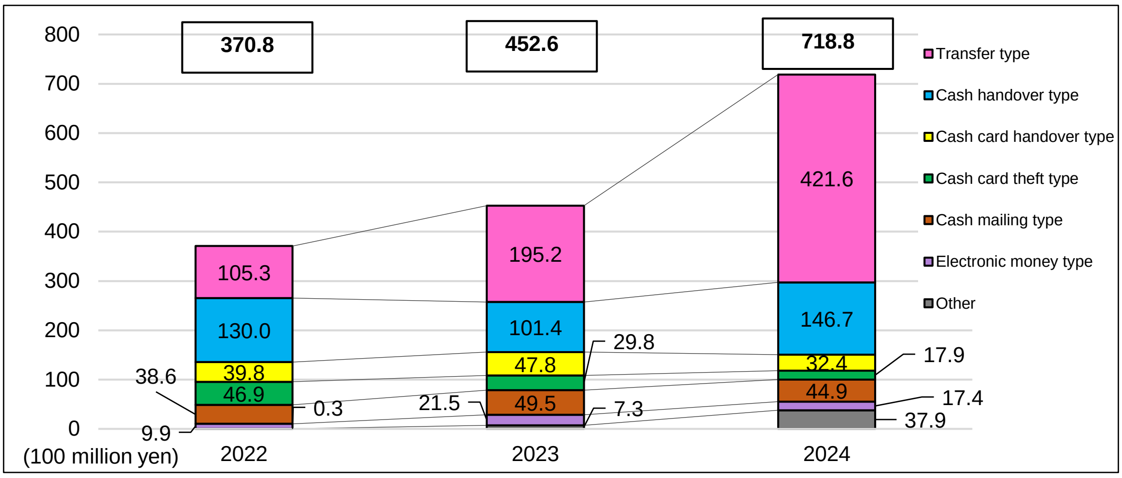


Table 30: Amount of Losses by Form of Payment



Note: As the figures are rounded to the nearest tenth, the total may not necessarily match the sum of the breakdown.

Anonymous and fluid criminal groups that commit online and telephone fraud recruit “ukeko”(cash collection operatives) and others by suggesting high financial rewards through social media and similar platforms, thereby inducing them to participate in the crimes. As a means of communication between the ringleaders, masterminds, and operatives, they often use highly anonymous communication tools equipped with functions that automatically delete messages, in an attempt to conceal evidence of their crimes.

Furthermore, in recent years, criminal groups committing online and telephone fraud are increasingly downsizing and diversifying their bases, such as scam operation bases, and relocating them at short intervals, with some cases using rented apartments and office spaces as operation bases. In addition, some cases have been observed where not only the ringleaders and masterminds, but also the callers and call centers themselves are located overseas.

In 2024, a total of 50 suspects were arrested by prefectural police after foreign authorities cracked down on scam operation bases such as call centers located overseas and the suspects were transferred to Japan (see Table 31).

Table 31: Status of Cleared Cases of Online and Telephone Fraud Suspects Involving Scam Operation Bases Overseas in 2024

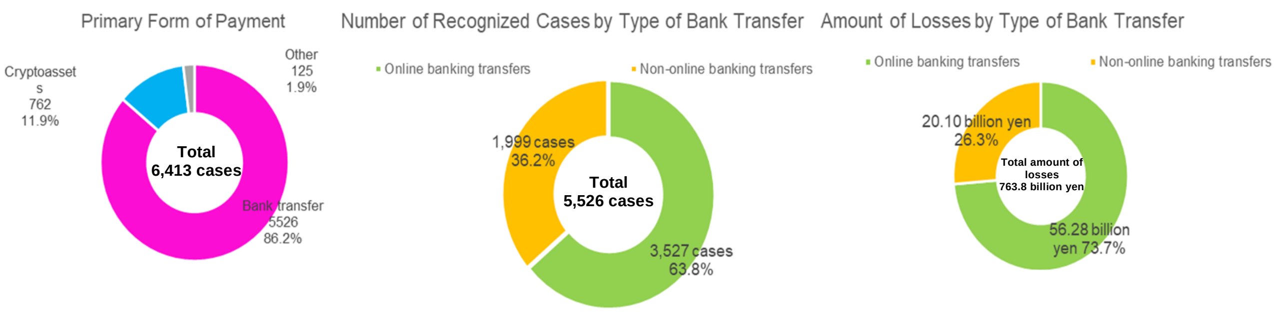
Country Name	Number of offenders arrested (people)
Cambodia	28
Philippines	14
Vietnam	6
Thailand	2

(C) Investment /romance fraud via social media

Investment /romance fraud via social media involve contacting victims through social media or matching apps, then shifting communication to another social media platform to build trust through repeated interactions, ultimately deceiving victims into transferring money to deposit/savings accounts. It is assessed that these schemes are carried out in an organized manner by anonymous and fluid criminal groups, with operational bases established for "Uchiko" (online contact operatives) who repeatedly communicate with victims on social media.

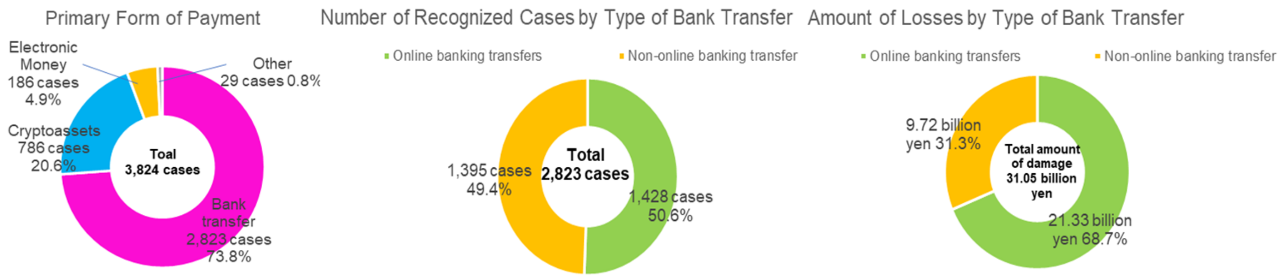
In 2024, the primary form of payment in investment fraud via social media were bank transfers of 5,526 cases (86.2%) and cryptoassets of 762 cases (11.9%), with bank transfers accounting for nearly 90% of the total. Of the bank transfers, 3,527 of the recognized cases involved the use of online banking, with a total amount of losses of 56.28 billion yen. These represented 63.8% of the recognized cases and 73.7% of the total amount of losses from all bank transfers.

Table 32: Primary Form of Payment in Investment Fraud via Social Media



In 2024, the number of recognized cases of romance fraud via social media by primary form of payment was 2,823 cases (73.8%) involving bank transfers and cryptoassets of 786 cases (20.6%) involving cryptoassets. Of the bank transfers, 1,428 of the recognized cases involved the use of online banking, with a total amount of losses of 21.33 billion yen. These represented 50.6% of the recognized cases and 68.7% of the total amount of losses from all bank transfers.

Table 33: Primary Form of Payment in Romance Fraud via Social Media



In investment/romance fraud via social media, bank transfers are the most common form of payment, with particularly large amount of losses resulting from transfers using online banking.

(D) Organized Theft and Trafficking of Stolen Goods

Organized theft and trafficking of stolen goods have been observed as a source of income for illegal foreign residents. In addition, cases have been confirmed where ringleaders located overseas instruct perpetrators, connected through social media and other platforms, on what items to steal and have large quantities of stolen goods sent to designated locations.

The police are advancing investigations into the actual situation, considering the possibility that Anonymous and fluid criminal groups are involved in organized theft and trafficking of stolen goods. They are also promoting comprehensive measures, including investigation and deterrence, in a unified and robust manner, such as by establishing cross-departmental project teams.

In light of the increasing trend of metal theft, including the theft of metal cables from solar power generation facilities, the Act on the Prevention of the Disposal of Stolen Specified Metals (Act No. 75 of 2025) was promulgated in June 2025. The law requires those engaged in the business of purchasing specified metal scrap[*1] to comply with obligations such as notifying authorities of their specified metal scrap purchasing business, verifying the identities of sellers when purchasing specified metal scrap, and creating and retaining transaction records.

(E) Malicious Host Club Offences and Amusement-Related Offences in Bustling Areas and Nightlife Spots

At malicious host clubs, women are exploited by taking advantage of their affections, deliberately saddling them with large debts despite knowing that they will be unable to repay the debts, and then compelling them to work as prostitutes or at sex-related businesses. In some cases, host clubs collude with sex-related businesses and intermediary scout groups that link them, systematically exploiting women to generate illicit profits.

In light of the situation where such practices have become a social issue, in May 2025, the Act to Partially Amend the Act on Control and Improvement of Amusement Business (Act No. 45 of 2025), which includes the regulation of malicious business practices, was promulgated.

*1 Metal scrap consisting of metals (copper and other metals specified by government ordinance) for which there is a high need to prevent the theft of items manufactured using such metals

(F) Online Gambling Offences

Regarding online casinos, there are offenders involved in various roles, including operators, users, persons involved in payment methods, advertisers, and promoters. There are also a variety of payment methods, including credit cards, cryptoassets, and bank transfers.

"Non-store-based" online casinos accessed via smartphones and other devices have been widely identified as contributing to increased access to gambling and the accompanying problem of gambling addiction. Concerns have also been raised that such platforms may facilitate the outflow of Japan's national assets overseas and money laundering.

In addition, there are cases where Boryokudan or Anonymous and fluid criminal groups are involved as the actual operators or behind the scenes of gambling offences related to online casinos.

(G) Online Banking Fraud Cases

In recent years, online banking fraud cases have occurred using phishing techniques, in which emails or SMS messages are sent pretending to be from real companies, organizations, or government agencies, directing recipients to view a fake website (phishing site) designed to look like the company's website, and then illegally obtaining account information, credit card numbers, and other data from that phishing site. There have also been confirmed cases where Anonymous and fluid criminal groups are involved in the unlawful acquisition of account information and unauthorized fund transfers.

(H) commercial transaction scam by malicious remodeling businesses, etc.

In recent years, criminal acts by malicious remodeling businesses have been confirmed, such as targeting elderly people's homes, pretending to be door-to-door salespersons offering home repairs work, plumbing work, and other home improvement and remodeling services, intentionally damaging homes even when no damage was found, and then demanding high construction fees for repairs. These malicious acts are carried out repeatedly and continuously in an organized manner, and the proceeds may be a source of funding for Anonymous and fluid criminal groups.

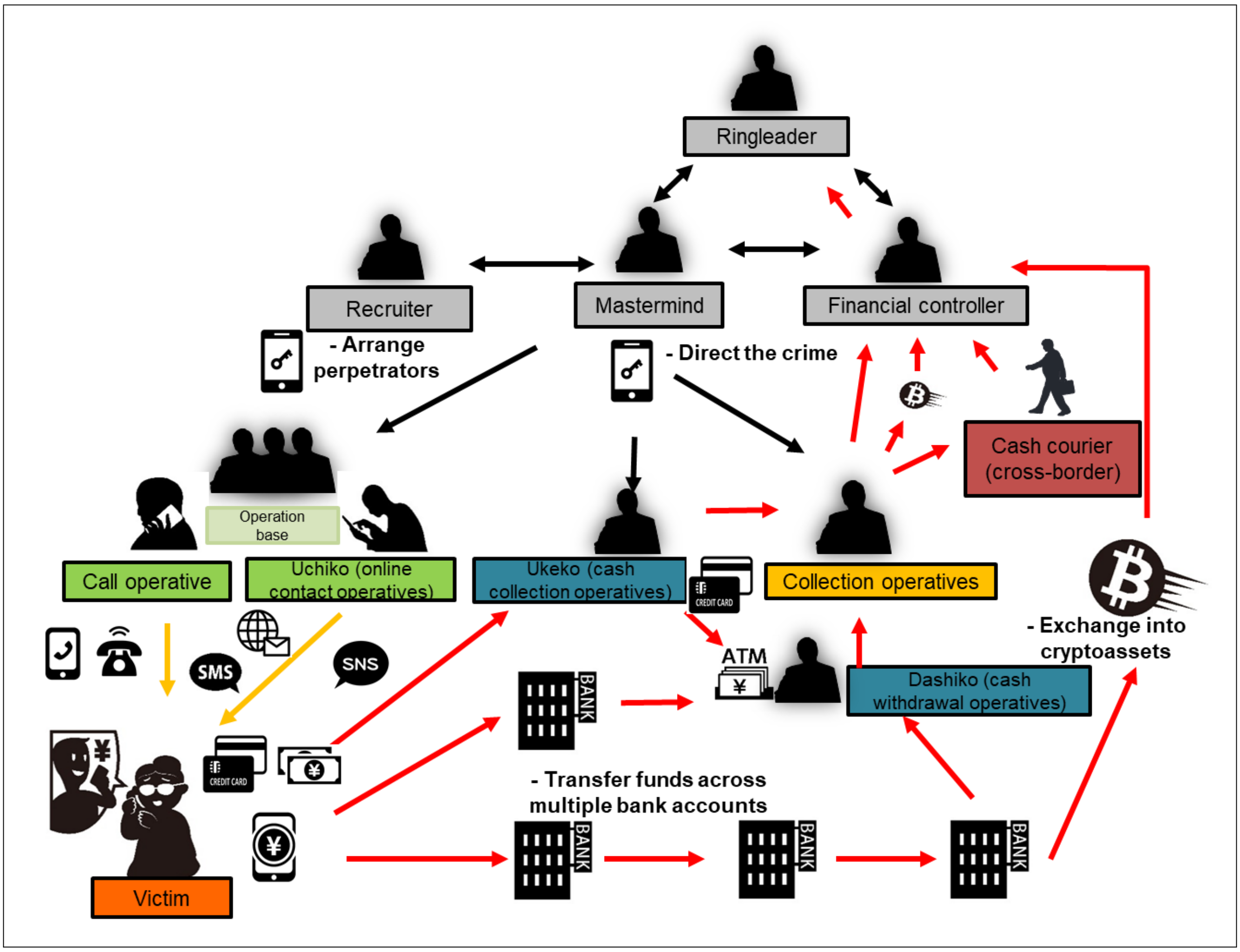
(iii) Modus Operandi of ML Offences Involving Anonymous and Fluid Criminal Groups

Modus Operandi of ML offences involving Anonymous and fluid criminal groups includes:

- Transfer money using fictitious or third-party accounts
- Transfer money to the bank accounts of cryptoassets exchange service providers and deposit the money into accounts managed by the suspect
- Transfer money to domestic accounts to exchange criminal proceeds in Japanese yen for foreign currency held by individuals
- Sell fraudulently obtained electronic gift cards through sites that mediate the buying and selling of such gift cards, and deposit the proceeds into accounts managed by the suspect
- Convert goods purchased using fraudulently obtained credit card information into cash by reselling them
- Sell goods that are criminal proceeds by impersonating others
- Use coin lockers to the convert of criminal proceeds
- Use vacant rooms to have victims send cash by mail and then receive it while posing as the intended recipient
- Conduct foreign remittances or transfers of cryptoassets
- Transfer criminal proceeds overseas through cash couriers (physical transportation of cash)

For example, when Anonymous and fluid criminal groups launder criminal proceeds obtained through online and telephone fraud, the flow of funds is illustrated in Table 34. The funds are believed to ultimately reach core members such as ringleaders, some of whom may be located at overseas bases.

Table 34: Actual Situation of Online and Telephone Fraud and Money Laundering by Anonymous and Fluid Criminal Groups (Illustration)



(2) Boryokudan

(i) Characteristics

In Japan, ML by Boryokudan remains a serious threat. Among cleared ML cases in 2024, 80 cases (6.2%) were related to Boryokudan members, associates, and other related parties (hereinafter referred to as "Boryokudan gangsters")

Table 35: Number of Cleared ML Cases Committed by Boryokudan Gangsters

Category \ Year	2022		2023		2024	
	Number of cases	Percentage to total (%)	Number of cases	Percentage to total (%)	Number of cases	Percentage to total (%)
Number of cleared cases by Boryokudan gangsters	64	8.8	57	6.3	80	6.2
Related to the Act on Punishment of Organized Crimes	62	8.7	54	6.1	71	5.6
Related to the Anti-Drug Special Provisions Act	2	11.8	3	14.3	9	42.9

Boryokudan repeatedly and continuously commit crimes to acquire funds, and shrewdly engage in ML.

The characteristics of revenue-generating by Boryokudan are as follows:

- Looking at the arrests of Boryokudan gangsters by major crime type, the proportion of fraud has fluctuated around 10%, but in 2024 it was a high 13.4%, indicating that revenue generating activities by fraud have become established.
- In recent years, Boryokudan gangsters have been deeply involved in online and telephone fraud in leading positions, suggesting that Boryokudan are using it as one of their major sources of funding.
- Revenue generating activities are conducted in a wide variety of areas, including finance, construction, labor dispatch, and adult entertainment businesses.

Table 36: Proportion of Boryokudan Gangsters among Offenders Arrested in Online and Telephone Fraud[*1] and Other Offences (2024)

	Number of Offenders Arrested in Online and Telephone Fraud and Other Offences (people)	Of which, Boryokudan Gangsters (people)	Proportion (%)
Offender	76	19	25.0
Mastermind of "Dashiko" (cash withdrawal operative) and "Ukeko" (cash collection operative)	36	14	38.9
Recruiter	163	54	33.1
Other	2,128	353	16.6
Total	2,403	440	18.3

An analysis ML cases committed by Boryokudan gangsters from 2022 to 2024 with a status of cleared revealed the following characteristics:

- By predicate offences, fraud, computer fraud, and theft were common.
- Regarding criminal proceeds subject to ML, the total amount (limited to those that can be monetized) was approximately 1.9 billion yen. As to the form, with cash including bank deposits accounting for approximately 80% of the cleared cases.

[*1] Refers to online and telephone fraud and investment/romance fraud via social media.

- When analyzed by transaction type, domestic exchange transactions accounted for more than 40% of all cases, while approximately 30% of cases involved receiving cash without involving any goods or services dealt with by deposit-taking institution.
- Looking at the accounts used by Boryokudan gangsters, over 80% were accounts under the names of fictitious or other parties, among which nearly 50% were in the name of relatives or acquaintances of Boryokudan gangsters.

  In other words, Boryokudan gangsters are conducting ML in ways that make tracing criminal proceeds difficult, such as:
- Receiving and transferring criminal proceeds in cash
- Misusing accounts in the names of relatives, acquaintances, or others to disguise the ownership of criminal proceeds

(ii) Typologies

The main cases of ML involving Boryokudan gangsters are as follows:

- The former Boryokudan gangsters illegally accessed online banking accounts, fraudulently transferred funds from third-party accounts to fictitious or other persons' accounts under control of the suspect, and then withdrew the cash.
- A Boryokudan gangster used bank accounts opened by other debtors at their direction, as well as accounts in the names of their relatives, as repayment accounts for illegal money lending operations.
- A former Boryokudan gangster instructed an accomplice to fraudulently obtain a loan from a financial institution under the pretense of borrowing business funds, thereby deceiving the institution out of money, and used bank accounts in the names of relatives and acquaintances.
- A Boryokudan gangster organized illegal gambling activities and had users transfer their betting money into bank accounts in the names of their relatives that they controlled.
- A Boryokudan gangster sold goods obtained through theft to a buyer by impersonating another person such as by providing a false name and converted them into cash.
- A Boryokudan gangster operated a sex-related business without the required license and had the proceeds obtained through customers' credit card payments transferred by a credit card payment agency into fictitious or third-party bank accounts under their control.
- A Boryokudan gangster knowingly received cash under the guise of so-called 'protection money' and similar payments while being aware that the funds constituted criminal proceeds derived from illegal gambling offences, prostitution offences, and the unlicensed operation of sex-related businesses, among other crimes.
- A Boryokudan gangster withdrew cash that had been transferred into fictitious or third-party accounts through online and telephone fraud, deposited the funds into an account in their own name, and then further transferred the money from that account to other accounts under their and their associates' control.

(3) Crime Groups of Foreigners*[1] in Japan

(i) Characteristics

With regard to foreign criminal groups operating in Japan, some are organized along lines of nationality or region of origin, while others—seeking to carry out crimes in a more sophisticated and efficient manner—repeatedly form and dissolve associations composed of members of various nationalities depending on the specific offense, reflecting a trend toward increasingly multinational organizational structures. In crimes involving such foreign groups in Japan, the transfer of criminal proceeds to other countries with different legal systems and financial transaction frameworks can make tracing those proceeds difficult. In recent years, there have also been numerous cases of transnational organized crime in which perpetrators in Japan commit theft, fraud, and other offences under instructions from masterminds based overseas, subsequently exporting stolen goods abroad or remitting criminal proceeds to foreign countries.

Looking at the clearance status of crimes committed by foreigners visiting or residing in Japan, both the number of cases cleared and the number of persons arrested in 2024 increased compared to the previous year. By nationality and related categories, Vietnam and China together accounted for approximately 60% of the total number of cleared cases and approximately 50% of the total number of persons arrested.

Table 37: Clearance Status of Crimes Committed by Foreigners in Japan by Nationality (2024)

	Number of Cleared Cases	
	Number of Cases (case)	Proportion (%)
Total	21,794	100.0
Vietnam	9,690	44.5
China	2,866	13.2
Thailand	1,201	5.5
Cambodia	991	4.5
Philippines	873	4.0
Brazil	830	3.8
Sri Lanka	667	3.1
Indonesia	605	2.8
Nepal	446	2.0
Korea	406	1.9
Other	3,219	14.8

	Number of Offenders Arrested	
	Number of Offenders (people)	Proportion (%)
Total	12,170	100.0
Vietnam	3,990	32.8
China	2,011	16.5
Philippines	732	6.0
Thailand	644	5.3
Brazil	578	4.7
Indonesia	484	4.0
Nepal	424	3.5
Sri Lanka	376	3.1
Korea	318	2.6
Cambodia	254	2.1
Other	2,359	19.4

Furthermore, of the ML cases cleared in 2024, 141 were committed by foreigners in Japan, accounting for 11.0% of the total.

Table 38: Number of ML Cases Cleared Involving Foreigners in Japan

Category \ Year	2022		2023		2024	
	Number of Cases	Percentage of the total (%)	Number of Cases	Percentage of the total (%)	Number of Cases	Percentage of the total (%)
Number of cases cleared involving foreigners in Japan	108	14.9	96	10.6	141	11.0
Number of cases cleared under the Act on Punishment of Organized Crimes	103	14.5	93	10.5	139	11.0
Number of cases cleared under the Narcotics Control Act (Special Provisions)	5	29.4	3	14.3	2	9.5

An analysis of status of cleared ML cases committed by foreigners visiting Japan from 2022 to 2024 revealed the

*1 "Foreigners in Japan" refers to non-permanent resident foreigners in the country, excluding settled residents (permanent residents, spouses of permanent residents, and special permanent residents), U.S. military personnel in Japan, and individuals with unclear residency status.

following:

- By nationality, the majority of offenders are from China and Vietnam, with China accounting for more than half of the total number of cleared cases.
- By predicate offences, fraud is the most common, followed by theft and computer fraud. In terms of the type of transaction, domestic exchange transactions are the most common, followed by credit card transactions.
- Looking at the accounts used by foreigners in Japan, approximately 70% were accounts under the names of fictitious or other parties.
- Looking at the cleared cases involving Chinese nationals by predicate offences, fraud is the most common, accounting for 41.2%, followed by theft at 37.4% and computer fraud at 12.6%. Looking at the cases by type of transaction misused, credit cards were the most common, accounting for 23.6%, followed by domestic exchange transactions at 11.8%.
- Looking at the cleared cases involving Vietnamese nationals by predicate offences, fraud is the most common, accounting for 36.4%, followed by theft at 20.3% and computer fraud at 14.4%. Looking at the cases by type of transaction misused, domestic exchange transactions were the most common, accounting for 39.7%, followed by credit cards at 11.1%.

As for the number of criminals arrested for illegal transfers of deposit books and cash cards in violation of the Act on Prevention of Transfer of Criminal Proceeds from 2022 to 2024, Vietnamese nationals accounted for approximately 70% of the total.

In addition, with respect to the number of STRs from 2022 to 2024, STRs related to Vietnamese and Chinese ranked the highest among other nationalities.

(ii) Typologies

(A) Chinese Nationals

There are approximately 870,000 foreign residents of Chinese nationality in Japan, accounting for about 23% of all foreign residents. Chinese criminal organizations often form groups by leveraging local or familial ties, or by recruiting colleagues from workplaces. There are also organizations such as the Chinese Dragon, primarily composed of children of Japanese nationals remaining in China after World War II, which have been expanding their influence mainly in the Tokyo metropolitan area. In recent years, there have also been cases where Chinese criminal organizations recruit residents via social media and assign them to carry out parts of criminal activities.

The following are examples of cleared ML cases involving Chinese nationals:

- Received goods purchased using fraudulently obtained credit card information by impersonating the cardholder.
- Created a counterfeit cash card using information obtained through skimming, and used it to transfer funds to fictitious or third-party accounts.
- Had the victim of a fraud transfer money into fictitious or third-party accounts under the suspect’s control, and then remitted the funds, including the defrauded amounts, to another person’s account under the guise of a private foreign currency exchange.
- Used fraudulently obtained electronic money rights by impersonating the rightful owner at the point of sale to purchase goods.
- At a courier company’s branch, presented a forged My Number card and impersonated a fictitious recipient to collect a package.

(B) Vietnamese Nationals

There are approximately 630,000 foreign residents of Vietnamese nationality in Japan[*1], accounting for about 17% of all foreign residents. By status of residence, the majority hold “Technical Intern Training,” “Specified Skilled Worker,” or “Engineer/Specialist in Humanities/International Services” visas, among others. Some individuals with problematic behavior have formed criminal groups through social media and other channels.

The following are examples of cleared ML cases involving Vietnamese nationals:

- Operated an underground banking service[*2] by using social media to accept requests for foreign remittances, having cash deposited into fictitious or third-party accounts in Japan, and then transferring amounts converted into the foreign currency from funds the suspect had pre-positioned abroad to accounts specified by the clients.
- Used fraudulently obtained online banking login credentials, and transferred funds from fictitious or third-party accounts under the suspect’s control to other fictitious or third-party accounts, and then withdrew the cash.
- Shipped stolen cosmetics and other items to a disposal agent with falsified descriptions and sender information on the shipping labels.

It has also become clear that Vietnamese nationals are involved in account-buying and selling networks, and in recent years, there has been a rising trend of account transactions conducted via social media. The accounts bought and sold are being misused in a variety of offences, including ML and online and telephone fraud.

(C) Other Foreigners in Japan

The following are examples of cleared ML cases involving other foreigners in Japan:

- Nigerian nationals and others deceived a U.S. company by sending emails containing false information, causing funds to be transferred into a corporate account opened in Japan, and made it appear as if the transfer was part of a legitimate transaction.
- Nigerian nationals and others deceived victims they met through social media, causing them to transfer money into fictitious or third-party accounts opened in Japan.
- Myanmar nationals operated an underground banking service by accepting requests for foreign remittances and having cash deposited into fictitious or third-party accounts opened in Japan.
- Filipino nationals caused funds obtained through online and telephone fraud to be transferred into fictitious or third-party accounts under the suspects’ control, and then withdrew the money on the same day using ATMs.
- Brazilian nationals used the payment system of a flea market app to record the proceeds from the sale of counterfeit branded goods within the app into an account in the name of a relative under the suspect’s control.

[*1] According to the Immigration Services Agency’s statistics on foreign residents (as of the end of December 2024). For the purposes of this report, ‘foreign residents’ refers to mid- to long-term residents and special permanent residents. The same definition applies to the items below.

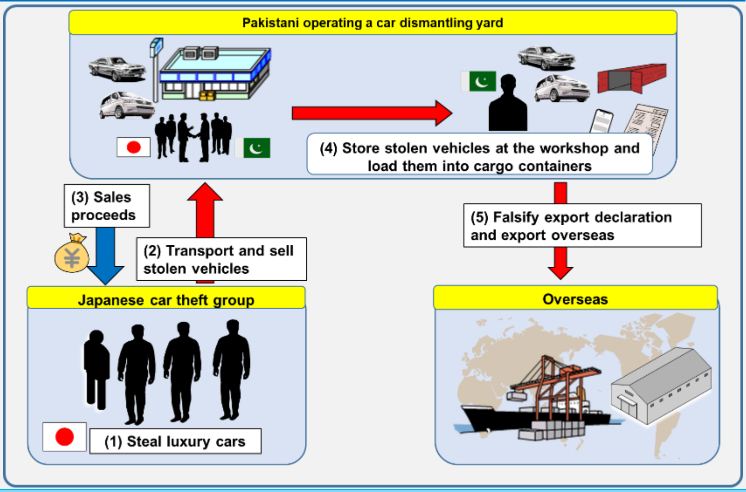
[*2] An underground banking service refers to a system in which a person without the required legal qualifications conducts foreign remittances for a fee, and such activity violates the Banking Act (Act No. 59 of 1981) and other related laws.

(D) Others (Cases of Illicit Export of Stolen Goods)

In recent years, there have been cases where foreign criminal groups in Japan have systematically carried out thefts and illicitly exported stolen goods abroad. Such cases are also observed to serve as a source of income for unlawfully residing foreigners and others.

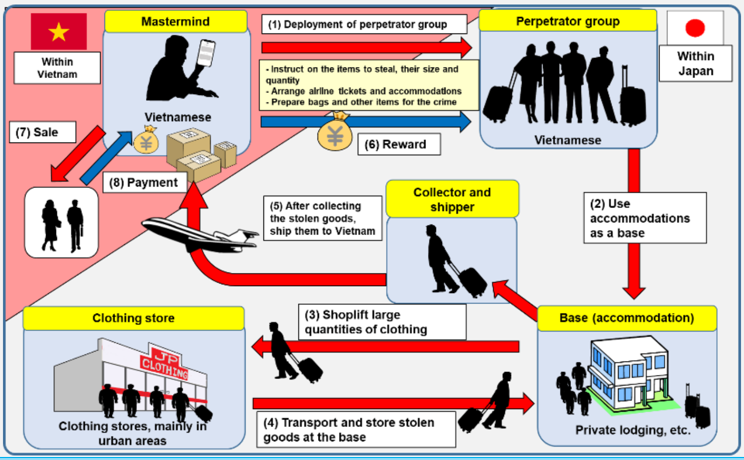
[Case of illicit automobile export involving a Pakistani national]

A Pakistani national operating a vehicle dismantling yard purchased stolen vehicles from a Japanese car theft group and stored them. The vehicles were then loaded into shipping containers and illicitly exported abroad with falsified export declaration information.



[Case of mass shoplifting targeting clothing stores by a Vietnamese group]

Under the direction of masterminds based in Vietnam, a Vietnamese group traveled to Japan and stole large quantities of clothing from clothing stores in a short period. The stolen goods were collected and shipped by collectors and shippers to Vietnam, where they were believed to have been sold.



2. Predicate Offences

(1) Major Predicate Offences

Money laundering refers to the concealment and receipt of proceeds obtained from certain predicate offences, as well as certain acts performed for the purpose of controlling the business management of companies, etc.

For the purpose here, “predicate offences” are defined as crimes under the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act. Predicate offences include offences that are committed with the intent of obtaining unlawful financial gain and those subject to the death penalty, imprisonment with work for life or four years or longer, or imprisonment without work offences listed in Tables 1 and 2 attached to the Act on Punishment of Organized Crimes, and drug-related offences listed in the Anti-Drug Special Provisions Act. Criminal Proceeds generated from such predicate offences are the primary source of the threat of ML/TF in Japan.

The number of cleared ML cases categorized as predicate offences in 2022–2024[*1] is as follows:

Table 39: Numbers of Cleared ML Cases under the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act (Categorized by Predicate Offence)

Year \ Predicate offences	Fraud	Theft	Computer fraud	Drug-related offences (Note 1)	Violation of the Investment Act/Money Lending Business Act (Note 2)	Habitual gambling/ running a gambling venue for profit	Violation of the Trademark Act (Note 3)	Violation of the Amusement Business Act	Document forgery offences (Note 4)	Extortion	Violation of the Immigration Control and Refugee Recognition Act	Violation of the Anti-Prostitution Act (see Note 5)	Embezzlement	Violation of the Financial Instruments and Exchange Act	Other	Total
2022	254	257	105	21	13	11	10	4	12	8	7	4	6	1	40	753
2023	334	319	160	22	16	17	9	9	9	5	6	5	6	6	32	955
2024	462	386	288	24	24	16	13	14	3	9	7	11	8	4	46	1,315
Total	1,050	962	553	67	53	44	32	27	24	22	20	20	20	11	118	3,023

Note 1: Drug-related offences refer to stimulant offences, cannabis offences, narcotics offences, psychotropics offences, and opium offences.
2: Money Lending Business Act (Act No. 32 of 1983)
3: Trademark Act (Act No. 127 of 1959)
4: Document forgery offences refer to the offences set forth in Articles 154 to 161.1 of the Penal Code.
5: Prostitution Prevention Act (Act No. 118 of 1956)

In recent years, the incidence of online and telephone fraud as well as investment/romance fraud via social media has increased, and many of these are carried out as revenue-generating activities by Anonymous and fluid criminal groups. As a result, the number of ML cases with these offences as predicate offences has also risen. In fact, looking at the total number of cleared cases by predicate offences from 2022 to 2024, as shown in Table 39, fraud and computer fraud together account for approximately 50% of the total.

[*1] There were 2,918 cleared ML cases under the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act from 2022 to 2024, while the total number of cleared ML cases counted by predicate offences was 3,023. This is because some ML cases that are counted under multiple predicate offences.

The comprehensive analysis of the primary predicate offences, examining the scale of criminal proceeds generated, their connection to ML offences, the types of transactions misused, and the potential risk of fascilitating organized crime is presented below.

(i) Fraud

(A) Forms of Offences and Criminal Proceeds

Frauds, including online and telephone fraud, investment/romance fraud via social media, are repeatedly and continuously committed by both domestic and foreign criminal groups, and generate large amounts of criminal proceeds using a variety of criminal tools, such as deposit/savings accounts under the names of fictitious or other parties or legal person's names.

In 2024, among crimes against property, the total amount of losses caused by fraud[*1] was the highest, reaching approximately 307.5 billion yen, representing an 89.1% increase compared to the previous year. There is also a trend of higher loss amounts per individual case.

(B) Money laundering cases

In ML cases with fraud as the predicate offence, there are cases where victims of online and telephone fraud or investment/romance fraud via social media are made to transfer money into fictitious or third-party accounts. In other cases, the defrauded funds are deposited into cryptoasset wallets of cryptoasset exchange service providers, after which accomplices purchase and transfer the cryptoassets.

[Case 1]
The suspect deceived a victim through a social media romance scam, causing funds to be transferred into their bank account. The suspect then sent the funds to a client account at a Cryptoassets exchange service providers they controlled and purchased cryptoassets, which was subsequently transferred to a cryptoasset wallet managed by the criminal group.

[Case 2]
The suspect acting as “Dashiko” (cash withdrawal operative), deceived victims through online and telephone fraud and had funds transferred into their bank account. The suspect then withdrew the money at ATMs and purchased electronic gift cards at multiple convenience stores. Afterwards, the suspect photographed the gift card codes and sent them to an email address managed by the criminal group.

(ii) Computer fraud

(A) Forms of Offences and Criminal Proceeds

In terms of computer fraud, one common method involves the suspect using IDs, passwords, or other credentials for online banking to gain unauthorized access to financial institutions’ systems, and then transferring funds from victim accounts to accounts under the suspect’s control. Another method involves using cash cards obtained through online and telephone fraud, either a third party operates an ATM to transfer funds into fictitious or third-party accounts, or the victim is instructed to operate an ATM to transfer funds into an account managed by the suspect (including refund frauds).

Although the total amount of losses from unauthorized transfers via online banking fraud in 2024 decreased compared to the previous year, they remained high at 8.69 billion yen.

[*1] This figure also includes the amount of losses from computer fraud.

(B) Money laundering cases

In ML cases involving computer fraud, there are cases where a person other than the account holder illegally operates online banking or payment apps to make transfers, as well as cases where victims are made to operate ATMs to send funds without being aware that they are making a bank transfer."

[Case 1]
The suspects impersonated police officers or prosecutors, telling victims that their accounts were being misused for criminal activities. They then elicited the victims' online banking login IDs, passwords, and other credentials, gained unauthorized access to the victims' accounts, and transferred funds from the victims' accounts to corporate accounts controlled by the criminal group.

[Case 2]
The suspects impersonated municipal office staff, convincing the victims that they were entitled to a medical fee refund and guiding them to ATMs to complete the refund procedure. The victims were made to operate the ATMs without being aware that they were making a bank transfer, and the funds were sent to fictitious or third-party accounts controlled by the criminal group.

(iii) Theft

(A) Forms of Offences and Criminal Proceeds

Theft takes various forms, including burglary, vehicle theft, and shoplifting. In addition, there are specialized forms such as cash card fraud where cash cards are stolen through methods like card swapping, and ATM withdrawal theft, in which stolen cash cards are used to withdraw money. These crimes are repeatedly and continuously carried out by Anonymous and fluid criminal groups, Boryokudan, and foreign criminal groups in Japan.

In recent years, there has also been a notable increase in metal theft, including the theft of metal cables from solar power generation facilities, with cases confirmed in which stolen items are sold to scrap metal buyers and similar businesses.

In 2024, the total amount of losses from theft amounted to approximately 78.9 billion yen (with amount of losses of cash of about 18.6 billion yen), generating substantial criminal proceeds.

(B) Money laundering cases

In ML cases with theft as the predicate offence, there are cases where stolen goods are sold to convert them into cash, or cash obtained through theft is deposited into deposit/savings accounts.

[Case 1]

The suspect used a cash card stolen through online and telephone fraud (cash card theft) to operate an ATM and transfer funds into fictitious or third-party accounts managed by the criminal group.

[Case 2]

The suspect sold metal cables stolen from a solar power generation facility to a scrap metal buyer by impersonating another person, including using a false name on the receipt, and converted the proceeds into cash.

(iv) Violation of the Investment Act/Money Lending Business Act

(A) Forms of Offences and Criminal Proceeds

Violation of the Investment Act/Money Lending Business Act includes so-called loan-shark crime[*1], in which loans are provided without proper registration and at excessively high interest rates. In such loan-shark crime, non-face-to-face solicitation methods are sometimes used, such as sending direct mail based on personal information described in lists of multiple-debtors, or recruiting large numbers of people via online advertisements or telephone calls. There are also cases where money is lent non-face-to-face and repayments are made via transfers to fictitious or third-party accounts.

In 2024, the total amount of losses from loan-shark crime amounted to approximately 4.5 billion yen, generating substantial criminal proceeds.

(B) Money laundering cases

In ML cases with loan-shark crimes as the predicate offence include the cases where:

- Repayments are made via transfers to fictitious or third-party accounts
- Repayments are made using credit card payments
- Lending and repayment are conducted under the guise of transactions of goods or similar activities.

Additionally, there are cases where bank accounts in the names of debtors, transferred to the lender in place of repayment, are misused as accounts to conceal illicit funds.

[Case 1]

The suspect operated a money lending business while posing as the operator of a flea market website, having customers pose as sellers of gift cards and transfer funds as purchase payments to receive loans. The suspect then arranged for gift cards equivalent to the loan amount plus illegally charged interest to be delivered and collected.

[*1] Meaning the cases of unregistered business operation and high interest rate offences (violation of the Money Lending Business Act (unregistered business operation) as well as the cases of violation of the Investment Act (high interest rates, etc.)) and offences related to loan shark (cases of violation of the Act on Prevention of Transfer of Criminal Proceeds related to money lending business, fraud, and violation of the Mobile Phone Wrongful Use Prevention Act).

(v) Habitual Gambling/Running a Gambling Venue for Profit

(A) Forms of Offences and Criminal Proceeds

Regarding offences related to habitual gambling and running a gambling venue for profit, there are various forms of gambling offences, such as gambling conducted through online casinos, in addition to hanafuda gambling, baseball gambling, and game-machine gambling. The reality is that, Boryokudan are deeply involved in gambling offences, either directly or indirectly, and gambling is an important source of funds for them.

With regard to online casinos, even if they are legally operated in a foreign country, accessing them from within Japan and gambling there is a crime, and there have been cleared cases in Japan, such as the following:

- Gamblers who accessed a website operated by a foreign company from within Japan and gambled were arrested on a simple gambling offence.
- An offender who had domestic gamblers access a website on a server installed in a foreign country from terminals installed in Japan and had them bet money was arrested for habitual gambling.
- An offender who developed a payment system compatible with online casinos and acted as a payment and collection agent for bets was arrested for aiding habitual gambling.

In the last three years, the number of issuance of temporary restraining order for confiscation before institution of prosecution prescribed by the Act on Punishment of Organized Crimes has been highest for gambling offences. In 2024, the orders for confiscation were issued against about 1.41 million yen in cash, which was the proceeds from habitual gambling for profit.

(B) Money laundering cases

ML offences involving habitual gambling/running a gambling venue for profit as a predicate offence include cases where suspects act as intermediaries to send payments for purchasing points used in online casino gambling, and transfer funds between multiple accounts to conceal the source of funds and the purpose of the transactions.

[Case 1]
The suspect, who acted as a payment and collection agent for an online casino, had casino players transfer payments for purchasing points for gambling into multiple corporate accounts under the suspect's control. The suspect then further transferred the criminal proceeds to other corporate accounts.

(vi)Violation of the Immigration Control and Refugee Recognition Act

(A) Forms of Offences and Criminal Proceeds

Examples of violations of the Immigration Control Act include cases where a foreigner forges a residence card for the purpose of giving an appearance of legitimacy when entering Japan, passing for a legal resident or a person with a valid work permit, etc.; cases where a foreigner possesses, uses, provides, or receives a forged residence card; cases where an offender forces a foreigner who does not have a work permit to work or arranges illegal employment for such a foreigner (hereinafter referred to as "promotion of illegal employment"). Regarding the promotion of illegal employment, there have been confirmed cases of trafficking in persons offences where an offender places foreigners under his/her control by taking away their passports, etc., and forcing them to work. In cases of forged residence card offences, it has been confirmed that, under the direction of masterminds based in China, various nationalities of residents, including Chinese nationals, were recruited to manufacture forged residence cards at bases established within Japan.

(B) Money laundering cases

ML offences involving a violation of the Immigration Control and Refugee Recognition Act as a predicate offence include cases where criminal proceeds are received under false pretenses for a transaction or disguised as legitimate business income.

[Case 1]
The suspect received a reward for introducing illegally residing foreigners as workers, disguising it as rent under a fictitious rental housing contract.

[Case 2]
The suspect arranged for foreigners to work as construction workers, an activity not permitted under their valid residence status, by placing them with multiple companies. Part of the revenue generated by these companies through the illegal labor activities of the foreigners, constituting criminal proceeds, was made to be transferred from the companies into the suspect's own account under the guise of management fees and other charges.

(vii) Violation of the Amusement Business Act/Violation of the Anti-Prostitution Act

(A) Forms of Offences and Criminal Proceeds

With respect to amusement-related offences such as violations of the Amusement Business Act or the Anti-Prostitution Act, the reality is that Boryokudan have been directly or indirectly involved in the violations committed by illegal amusement businesses or sex-related businesses (hereinafter, "amusement business, etc."). Examples include association with operators of amusement business, etc. Criminal proceeds from these offences are an important source of funds for them.

Furthermore, activities in bustling areas and nightlife spots, such as direct and indirect involvement in the management, scouting, and other operations of illegal amusement businesses, sex-related businesses, and other such businesses, are thought to be major sources of financing for anonymous and fluid criminal groups.

In the last three years, the number of issuance of preservation order for confiscation before prosecution prescribed by the Act on Punishment of Organized Crimes has been highest for those related to violation of the Amusement Business Act and the Anti-Prostitution Act. In 2024, there was a case where bank deposit claims of approximately 31.87 million yen, which were the proceeds made in violation of the Amusement Business Act, became subject to an order for confiscation.

(B) Money laundering cases

ML offences involving a violation of the Amusement Business Act or the Anti-prostitution Act as a predicate offence include the cases where proceeds obtained from unlicensed operations are transferred into accounts in the names of acquaintances and received by the suspect.

[Case 1]
The suspect settled the charges for an unlicensed restaurant offering entertainment service using a credit card terminal installed at another restaurant they managed. The sales proceeds from the restaurant offering entertainment service were received by having them transferred from the credit card payment agency into an account in the name of an acquaintance.

(viii) Trafficking in persons offences

(A) Forms of Offences and Criminal Proceeds

Trafficking in persons offences refers to any crime, regardless of its formal designation, involving the recruitment, transfer, or receipt of a person for the purpose of exploitation such as sexual exploitation, forced labor, or organ removal, using means such as violence, threats, abduction, or the exchange of money.

In 2024, there were 96 cleared cases of trafficking in persons offences. Among the 63 victims protected by the police, approximately 90% were Japanese nationals, and about 70% of the Japanese victims were under 18 years of age. Confirmed cases include cases where employees of host clubs were forced to solicit women customers for prostitution in order to collect accounts receivable.

Additionally, in 2024, for a case involving a violation of the Anti-Prostitution Act constituting a trafficking in persons offence, a confiscation judgment was issued for approximately 1.54 million yen in cash, representing criminal proceeds obtained through prostitution.

(B) Money laundering cases

In ML cases with trafficking in persons offences as the predicate offence, there are cases where criminal proceeds obtained through prostitution are transferred into accounts managed by the suspect.

[Case 1]
The suspect, as a member of a scout group that arranged employment at sex-related businesses, recruited women from across the country to work at such businesses. The suspect then received part of the revenue generated by the recruited women's activities at the businesses in cash by mail, under the guise of a scout commission.

[Case 2]
The suspect forced female patrons of a host club to work at private-room bath facilities and engage in prostitution in order to collect accounts receivable for their food and drink charges. The suspect then had the women transfer the proceeds from the prostitution, knowing they were criminally obtained, into an account managed by the suspect.

(ix) Investment Fraud (Violation of the Financial Instruments and Exchange Act.etc)

(A) Forms of Offences and Criminal Proceeds

In investment frauds, including violations of the Financial Instruments and Exchange Act, there have been cases that advertised investment in foreign investment operators or cryptoasset trading, as well as cases where process from the solicitation to contract conclusion for financial products are conducted entirely online. As the times change, the products and tactics used in offences are undergoing transformation.

In 2024, the total amount of losses from investment fraud offences amounted to approximately 177.6 billion yen, generating substantial criminal proceeds.

(B) Money laundering cases

ML offences involving investment fraud as a predicate offence include the cases where stock transfer payments or investment funds are transferred into accounts managed by the suspect under the guise of a legitimate purpose.

[Case 1]

Despite not being registered as a Type I financial instruments business operator, the suspect bought and sold stocks on behalf of clients. When receiving the proceeds from the stock transfers, the suspect had the funds transferred into an account in the name of a general incorporated association under their control and sent donation receipts to the clients, thereby disguising the funds as donations.

[Case 2]

Despite not being registered as a Type II financial instruments business operator, the suspect solicited funds from clients under the pretext of investing in a business selling PCR test kits. The suspect executed loan agreements for the investment funds, making them appear to be loans, and had the money transferred into their own account.

(x) Drug-related Offences

(A) Forms of Offences and Criminal Proceeds

The drug-related offences in Japan exhibit the following characteristics.

- The quantities of drugs seized overall and those siezeded from smuggling offences (see Table 40), drug smuggling and trafficking continue to generates large amounts of criminal proceeds.
- The number of cases in which individuals were arrested for importing stimulants in 2024 was 101, a decline compared with the previous year.
- Among persons arrested for profit-driven stimulant offences(see Table 41), around 40% were members of Boryokudan gangsters, and about 20% were foreigners, indicating the involvement of Boryokudan and foreign criminal organizations.
- Criminal proceeds generated from drug trafficking or smuggling are likely to be transferred across borders between jurisdictions with differing legal and financial-transaction frameworks.
- The number of preservation order for confiscation issued before prosecution made under the Anti-Drug Special Provisions Act in 2024 was 27. The assets covered by these orders included monetary claims totaling approximately 23.91 million yen, as well as foreign currency. In the past, automobiles, land, and buildings have also been targeted, showingthat criminal proceeds obtained in cash are transformed into another type of property.

Table 40: Trends in Amounts Seized and the Amounts Seized from Smuggling by Drug Type

	Amount seized			Amount seized for smuggling		
	2022	2023	2024	2022	2023	2024
Stimulants (kg)	289.0	1,342.9	1,409.0	282.1	1,215.5	1,379.8
Dried cannabis (kg)	289.6	784.5	318.0	13.9	370.4	77.2
Cannabis concentrate (kg)	74.0	35.7	67.6	70.2	30.9	61.5

Note: The amount of stimulants seized (kg) does not include tablet-type stimulants.

Table 41: Status of Cleared Cases of Profit-driven Offences by Type of Drug-related Offence

			2022	2023	2024
Stimulant offences	Number of offenders arrested		450	603	516
		Boryokudan gangsters	191	220	221
		Percentage (%)	42.4	36.5	42.8
		Foreigners	97	170	108
		Percentage (%)	21.6	28.2	20.9
Cannabis offences	Number of offenders arrested		436	550	467
		Boryokudan gangsters	105	112	84
		Percentage (%)	24.1	20.4	18.0
		Foreigners	40	71	66
		Percentage (%)	9.2	12.9	14.1

(B) Money laundering cases

ML offences involving drug-related offences as a predicate offence include the cases where criminal proceeds from drug sales are transferred into accounts under the name of fictitious or other parties for the purpose of concealing and receiving them, as well as the cases where these proceeds were remitted to foreign countries using payment systems on flea market apps or funds transfer services.

[Case 1]

The suspect, in selling psychotropic drugs, disguised them as other products and listed them on a flea market app to appear as legitimate transactions, receiving the payment through the app's payment system.

(2) Predicate Offences of International Concern

The FATF urges countries to develop legal frameworks that comprehensively cover a wide range of offences as predicate offences for ML. While the direct connection to ML is limited in Japan, there are offences that are considered major predicate offences in other countries and are internationally recognized as of concern. Therefore, it analyzes the situation regarding these offences in Japan[*1].

(i) Bribery and corruption

(A) Forms of Offences and Criminal Proceeds

Bribery and corruption involving senior officials of the national or local governments fundamentally undermine public trust in Japan's society and economy. In 2024, the Prefectural Police have cracked 28 bribery cases. Additionally, in 2024, a case of aggravated bribery resulted in a supplementary confiscation judgment of 1.1 million yen.

[*1] In the "Report on the State of Effectiveness and Compliance with the FATF Standards" published by the FATF in April 2022, the most frequently identified major predicate offences for ML in mutual evaluation reports of various countries were, in order, drug trafficking, corruption, fraud, and tax crimes.

Looking at the Corruption Perceptions Index (CPI)[*1], one of the international indicators recommended by the FATF in its guidance for assessing corruption risk, Japan ranked 20th out of 180 countries in 2024, indicating a relatively low risk of corruption on an international scale.

(B) Money laundering cases

ML offences involving bribery and corruption as a predicate offence include the cases where bribe money is transferred into accounts in the names of third parties or received under false pretenses.

[Case 1]
The suspect, when receiving a bribe, had the money sent by registered cash mail to an acquaintance who was unaware of the circumstances and received it that way.

[Case 2]
The suspect received part of the bribe money under the guise of a salary.

(ii) Tax Evasion

(A) Forms of Offences and Criminal Proceeds

Tax evasion is a crime in which a taxpayer avoids paying taxes or obtains a tax refund through falsehoods or other fraudulent acts.

Tax evasion cases involve violations of laws such as the Consumption Tax Act (Act No. 108 of 1988), the Income Tax Act (Act No. 33 of 1965), and the Corporation Tax Act (Act No. 34 of 1965), with the applicable law depending on the type of tax involved.

In recent years, with the globalization of economic and social activities, cross-border transactions have come to be conducted on a continuous basis, and the forms of asset holding and management have become increasingly complex and diversified. Against this backdrop, cases have been identified in which tax evasion was carried out through the use of foreign entities, as well as international tax evasion in which funds were concealed overseas.

In fiscal year 2024, the National Tax Agency referred 98 cases to the Public Prosecutors Office, with the total amount of tax evasion involved in these criminal tax investigation cases estimated at approximately 8.2 billion yen.

In Japan, regardless of whether a case is subject to criminal prosecution, the tax authority conducts investigations and, if underreporting or non-filing is confirmed, impose additional taxes as an administrative sanction on top of the taxes owed. For those who fail to pay voluntarily, the authority enforces collection measures such as property seizure to ensure proper recovery of tax claims.

(B) Money laundering cases

ML offences involving tax evasion as a predicate offence include the following cases:

[*1] The index published annually by the international non-governmental organization Transparency International

[Case 1]

The suspect, in order to conceal criminal proceeds obtained from illicit export transactions, executed a loan agreement with the trading company and transferred the funds into an account in the company's name as a short-term loan.

(iii) Environmental Offences

(A) Forms of Offences and Criminal Proceeds

Environmental offences include waste-related offences and animal/bird-related offences. In 2024, there were 4,719 cleared cases for waste-related offences (decreased by 335 from the previous year) and 724 cases for other environmental offences[*1] (decreased by 54 from the previous year).

Although not considered predicate offences, there has been a recent increase in organized and wide-ranging poaching of coastal resources, such as abalone and sea cucumbers, in violation of fisheries laws and regurations[*2]. In 2023, the nationwide number of poaching cleared cases by the Japan Coast Guard, prefectural police, and prefectural authorities was 1,716 cases (increased by 155 from the previous year).

(B) Money laundering cases

ML offences involving environmental offences as a predicate offence include the following cases:

[Case 1]

The suspect operated an industrial waste disposal business without a license and received criminal proceeds obtained from contracting to transport and dispose of industrial waste generated by facility construction and other works, having the clients transfer the funds into an account in the name of an acquaintance.

[*1] Other environmental offences include violations of the Forest Act (Act No. 249 of 1951), the Act on Recycling of Materials Used in Construction Work (Act No. 104 of 2000)), and the Water Pollution Prevention Act (Act No. 138 of 1970), as well as animal/bird-related crimes such as violations of the Act on Welfare and Management of Animals (Act No. 105 of 1973) and the Act on the Protection and Management of Wildlife, and the Optimization of Hunting (Act No. 88 of 2002).

[*2] This refers to the Fishery Act (Act No. 267 of 1949), the Act on the Protection of Marine Resources (Act No. 313 of 1951), the Act on the Regulation of Fishing Operations by Foreign Nationals (Act No. 60 of 1967), and related laws.

3. Major Transactions Misused for Money Laundering

(1) Major Transactions Misused for Money Laundering

FATF guidance (National Money Laundering and Terrorist Financing Risk Assessment) states that when assessing risk, it is useful to consider three stages of ML[*1]. Based on the intent of this guidance, the police in Japan analyzed cleared ML/TF cases to examine what transactions were misused for ML/TF,

Specifically, they summarized the transactions, products and services that were misused for concealment and receipt of criminal proceeds, as well as products and services that were misused for transforming criminal proceeds obtained in the predicate offences, to the extent revealed in the course of the investigation.

The results of the analysis for the three years from 2022 to 2024[*2] are shown in Table 42.

Table 42: Major Transactions Misused for ML

Misused transaction / Year	Domestic exchange transactions(Note 1)	Cash transactions Sale (Sale of stolen goods, etc.) (Note 2)	Credit cards	Prepaid payment instruments (Note 3)	Deposit transactions	Cryptoassets	Legal persons	Funds transfer services	Cross-border transaction (such as foreign exchanges)	Financial instruments	Precious metals and stones	Electronic payment instruments (Note 4)	Real estate	Money lending	Foreign currency exchange	Legal/accounting professionals	Bills and checks	Postal receiving services	Total
2022	266	80	55	39	24	16	6	10	7	0	1	-	0	0	0	1	0	0	505
2023	311	89	51	40	36	29	15	21	11	3	3	-	4	2	2	0	1	1	619
2024	551	101	73	36	29	43	35	10	5	4	2	6	1	2	1	1	0	0	900
Total	1,128	270	179	115	89	88	56	41	23	7	6	6	5	4	3	2	1	1	2,024

Note 1: Exchange transactions (undertaking customer-requested transfers of funds using a system for transferring funds between distant locations without directly transporting cash) comprise one of the services provided by banks and other deposit-taking institutions. Here, domestic remittances (excluding deposits, withdrawals, and the use of bills and checks) through deposit-taking institutions are counted as domestic exchange transactions.

2: In this report, for cases where both cash transactions and deposit transactions were exploited, they are not counted under cash transactions but are counted only under deposit transactions.

3: Since 2023, the name “electronic money” has been changed to “prepaid payment instruments” in the NRA-FUR.

4: In this report, electronic payment instruments are counted.

The results of the analysis of the cleared ML cases and STRs over the three years from 2022 to 2024 are as follows:

[*1] (i) Placement: The stage at which criminal proceeds enter the financial system. (ii) Layering: The stage where criminal proceeds are separated from their source of funding to make their origin opaque. (iii) Integration: The stage at which criminal proceeds are injected into legitimate economic activities.

[*2] The goods and services tabulated are limited to those related to goods and services handled by specified business operators (excluding cash transactions).

- There were 1,128 cases of domestic exchange transactions, followed by 89 cases of deposit transactions, with approximately 60% of that transactions misused for ML involving products and services offered by deposit-takinginstitutions.
- Amid a significant increase in cases where offenders have victims make payment to bank accounts opened in the name of fictitious or other parties through domestic exchange transactions, which enables prompt and secure fund transfers, there has also been a growing trend in the misuse of accounts held in the names of corporations with no real substance or with opaque operations.
- Criminal proceeds deposited into accounts through domestic funds transfers are often converted into cash or exchanged for cryptoassets, making subsequent tracing difficult.
- In cases involving the misuse of cash transactions, the majority involve converting criminal proceeds, such as stolen goods, into cash by selling them to buyers.
- The number of cases where credit cards were misused for ML was the third highest and has remained at a high level. The majority involve the fraudulent use of credit cards for ML, such as impersonation.
- In addition to the continued misuse of prepaid payment instruments, cryptoassets, and funds transfer services, since 2024, the misuse of electronic payment instruments has also been observed. This indicates that new products and services are increasingly being misused, reflecting the diversification of payment methods.

In addition, in ML schemes, there are many cases that are carried out without using the products and services of specified business operators. Examples of cases that do not involve products and services of specified business operators include the following:

- Physically hiding criminal proceeds from online and telephone fraud or theft in coin lockers or similar locations
- Receiving cash that constitutes criminal proceeds from online and telephone fraud, and then handing it over to another person
- Mailing criminal proceeds while impersonating another person, as well as receiving mailed criminal proceeds using vacant rooms or delivery lockers while impersonating someone else

(2) Measures to combat crimes facilitating the misuse of deposit/savings accounts

In ML cases, fictitious or third-party accounts (including online accounts) serve as a primary criminal infrastructure.

The police are actively cracking down on activities that promote the misuse of deposit/savings accounts, including:

- Violation of the Act on Prevention of Transfer of Criminal Proceeds related to the unauthorized transfer of passbooks, cash cards, and other deposit-related instruments
- “Account fraud,” in which, with the intent to transfer to another person, individuals falsely provide the address of a postal receiving service provider as their residence when opening an account, thereby fraudulently obtaining passbooks or other deposit instruments from financial institutions
- “Receipt of stolen property,” in which individuals knowingly receive passbooks or other deposit instruments obtained by fraud. (See Tables 43 and 44.)

Looking at the number of cleared cases for violation of the Act on Prevention of Transfer of Criminal Proceeds by the nationality of the suspects, Japan accounts for the highest number, followed by Vietnam and China. In cases involving the misuse of accounts in the names of foreigners, schemes have been observed in which monetary deposits are made into deposit/savings accounts fraudulently transferred by foreign residents returning to their home countries, after which cash is withdrawn or funds are transferred to other accounts while impersonating the original account holders.

Furthermore, in recent years, ML schemes using deposit/savings accounts have expanded beyond the physical transfer of passbooks and other deposit instruments. Schemes have been observed in which individuals provide others with the numbers and branch names of their own accounts, have funds deposited into these accounts, and then transfer the money from these accounts to designated separate accounts.

In light of this situation and the various cases observed, it can be inferred that the number of transferred accounts far exceeds the number of cleared cases. Attention must be paid to the fact that the transfer of accounts promotes the execution of ML and other criminal activities.

Table 43: Number of Cleared Cases of the Violation of the Act on Prevention of Transfer of Criminal Proceeds

Category \ Year		2022	2023	2024
Transfer of passbooks and other deposit instruments	(cases)	2,951	3,230	4,321
Transfer of passbooks and other deposit instruments (business)	(cases)	18	43	29
Solicitation or inducement for the transfer of passbooks and other deposit instruments	(cases)	10	12	12
Transfer of foreign exchange transaction cards and similar instruments	(cases)	41	50	60
Provision of information for cryptoasset exchanges	(cases)	46	89	90
Other	(cases)	0	0	1
Total	(cases)	3,066	3,424	4,513

Table 44: Number of Cleared Cases of Account Fraud and Other Offences

Category \ Year		2022	2023	2024
Account Fraud	(cases)	733	726	907
Receipt of stolen goods	(cases)	0	3	0
Total	(cases)	733	729	907

Note: The figures include cases reported by prefectural police to the National Police Agency as offences that facilitate online and telephone fraud.

The police promptly suspend the use of accounts that have been used in online and telephone fraud, preserve the victims' assets, and, to prevent the same accounts from being used in further crimes, request account freezes from financial institutions managing the accounts whenever losses from online and telephone fraud or similar crimes is recognized. Financial institutions receiving such information from the police are required to implement account freeze measures in accordance with the Act on Damage Recovery Benefit Distributed from Fund in Bank Accounts Used for Crimes (Act No. 133 of 2007).

There have been confirmed cases where corporate representatives submitted applications for the attachment of claims to the court based on false payment demands or notarized deeds and withdrew funds from the frozen accounts through compulsory execution. The frozen accounts in these cases were foreign or corporate accounts into which funds fraudulently obtained through investment scams had been deposited. In relation to these cases, the corporate representatives who submitted the applications for attachment of claims have been prosecuted for fraud and for making false statements in, and using, notarized deeds.

[Topic] APG Yearly Typologies Report 2024

APG*1 annually collects information from participating countries on ML schemes, trends, and related matters, and publishes the results as the "Yearly Typologies Report" (hereinafter, the "Report"). Each year, the Report covers specific topics; in 2023, it focused on "cryptoassets," and in 2024, on the "misuse of legal persons."

In the Report published in November 2024, the situation regarding ML in the Asia-Pacific region is described as follows:

[Special Feature: Misuse of Legal Persons]

1. Purposes of Misuse of Legal Persons

The purposes for which legal persons are misused are diverse and include the following:

- To give the appearance that those involved are distanced from the criminal activity
- To conceal the true ownership of assets (including those owned by Politically Exposed Persons, PEPs).
- To provide legitimate business reasons for the transfer of large sums of money
- To commingle criminal proceeds with legitimate funds
- To spend or invest criminal proceeds
- To facilitate corruption, fraud, and tax evasion
- To transfer bribes or embezzled public funds
- To protect assets acquired using criminal proceeds.

2. Recent Trends in the Misuse of Legal Persons

Many APG member countries/regions have commonly reported that legal persons are being misused to facilitate offences such as fraud via email or telephone, investment fraud, and Business Email Compromise (BEC), as well as tax evasion.

Other predicate offences where the misuse of legal persons has been observed include theft, embezzlement, bribery and corruption, securities and market manipulation, smuggling, drug trafficking, and the distribution of obscene materials. Legal persons have also been reported to be misused for ML, particularly Trade-Based Money Laundering (TBML).

Methods of the misuse of legal persons include the use of shell companies, the appointment of nominee directors or other figurehead officers, the movement and commingling of funds through business accounts, and the structuring of lending transactions.

3. Beneficial Ownership

The purpose of concealing the beneficial ownership is straightforward: to prevent the true owner of assets or proceeds from being linked to those assets or their source. Concealment of the beneficial ownership can lead to the non-reporting of taxable income and hinder confiscation and recovery proceedings. This applies universally to all predicate offences and ML.

Moreover, complex legal structures involving companies or trusts often span multiple jurisdictions, a characteristic commonly observed in tax crimes and related ML schemes. For example, such legal structures are used to obscure the true controllers of vessels or companies involved in illegal fishing.

*1 Asia/Pacific Group on Money Laundering. It is an organization established to strengthen and promote measures against ML/TF in Asia-Pacific jurisdictions that are not members of the FATF. The organization provides support and assistance to countries/regions working to enhance their ML/TF frameworks. As of the end of June 2025, a total of 42 countries/regions, including Japan, participate in the organization.

4. Suspicious Transaction Report (STR)

(1) Overview and Reporting Status

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators (excluding lawyers[*1], etc. and judicial scriveners[*2], etc. [*3]) to submit STRs to competent authorities if assets received in transactions related to specified business affairs[*4] are suspected of being criminal proceeds, or if there is suspicion of ML in connection with transactions related to specified business affairs. The Act also requires specified business operators to determine if there is such suspicion by considering the transaction type and other matters when conducting verification at the time of transactions as well as the details of the NRA-FUR and by using the method set forth in the ordinance of the competent ministry.

In addition, competent authorities have formulated *the List of Reference Cases of Suspicious Transactions*[*5] that illustrates patterns of transactions that may be suspicious and require special attention, taking into account the characteristics of the business of the specified business operators, and have published the list on the website. The "List of Reference Cases of Suspicious Transactions" is updated as appropriate in response to changes in criminal methods and amendments to relevant laws and regulations.

Against the backdrop of heightened awareness of anti-money laundering and related measures across Japan and the advancement of monitoring systems among specified business operators, the number of STRs has been on an upward trend. In 2024, the number of suspicious transaction notifications[*6] reached 849,861.

Looking at the number of STRs by business type, the percentage of STRs reported by banks and other deposit-taking institutions was the largest, accounting for 71.9% (611,069) of the total STRs, followed by money lenders at 10.39% (88,282) and credit card operators at 6.82% (57,978) (see Table 45). Meanwhile, with respect to specified business operators in the non-financial sector, such as real estate agents, dealers in precious metals and stones, and postal receiving service providers, the number of STRs has increased; however, their overall share of the total remains low.

With regard to the quality of STRs, those that specifically describe the grounds for suspicion and are accompanied by supporting materials such as transaction statements are useful for analysis and investigation and are considered to be high-quality reports[*7*8].

[*1] Persons listed in Article 2, paragraph (2), item (xlv) of the Act on Prevention of Transfer of Criminal Proceeds (lawyer or legal professional corporation. Referred to as "lawyers, etc." in this NRA-FUR.)

[*2] Persons listed in Article 2, paragraph (2), item (xlvi) of the Act on Prevention of Transfer of Criminal Proceeds (judicial scrivener or judicial scrivener corporation. Referred to as "judicial scriveners, etc." in this NRA-FUR.)

[*3] The amended Act on Prevention of Transfer of Criminal Proceeds, pursuant to the FATF Recommendation Compliance Act (the Act to Partially Amend the Act on Special Measures Concerning Asset Freezing of International Terrorists Conducted by Japan Based on United Nations Security Council Resolution 1267, etc. (Act No. 97 of 2022)) which was promulgated in December 2022, came into effect on April 1, 2024. The amendment stipulates that persons listed in Article 2, paragraph (2), item (xlvii) of the Act (certified administrative procedures legal specialist or certified administrative procedures legal specialist corporation. Referred to as "certified administrative procedures legal specialists" in this NRA-FUR), persons listed in Article 2, paragraph (2), item (xlviii) of the Act (certified public accountant or audit corporation. Referred to as "certified public accountants" in this NRA-FUR), and persons listed in Article 2, paragraph (2), item (xlix) of the Act (certified public tax accountant or certified public tax accountant corporation. Referred to as "certified public tax accountants, etc. " in this NRA-FUR) are required to submit STRs, except for matters pertaining to the confidentiality obligations.

[*4] Meaning the specified business set forth in Article 4, paragraph (1) of the Act on Prevention of Transfer of Criminal Proceeds.

[*5] These cases are provided as a reference for specified business operators to detect or extract suspicious transactions in the course of their daily transactions. While not all cases that formally match these cases are suspicious transactions, it should be noted that even transactions that do not match these cases will be subject to reporting if the specified business operator judges them to be suspicious transactions. When specified business operators submit STRs, they are required to fill in the guideline numbers and names in Guidance for Submitting STRs to indicate which reference case the transaction mainly falls under.

[*6] The number of notifications received by the National Public Safety Commission and the National Police Agency from the competent authorities concerning matters related to STRs.

[*7] The characteristics of ML and related activities involving ransomware, as well as key points to consider when filing STRs, are described in the 2024 Survey Report under "[Topic] ML/TF related to Ransomware."

[*8] The characteristics of cyber enabled fraud and key points to consider when filing STRs are described in the 2024 Survey Report under "[Topic] Flow of Criminal Proceeds from Cyber Enabled Fraud (CEF)."

Table 45: Annual Reported Number of STRs by Business Type

Category \ Year			2022	2023	2024		
			Number of reports	Number of reports	Number of reports	Share of the total (%)	Year-on-Year (%)
Financial institutions			542,003	661,838	791,440	93.13	+19.6
	Deposit-taking institutions		435,728	522,649	611,069	71.90	+16.9
		Banks (Note 1)	414,651	498,155	580,382	68.29	+16.5
		Shinkin banks, credit cooperative	18,520	21,636	24,925	2.93	+15.2
		Labour banks	316	397	1,370	0.16	+245.1
		Norinchukin banks, etc.(Note 2)	2,241	2,461	4,392	0.52	+78.5
	Insurance companies		3,939	4,575	5,428	0.64	+18.6
	Financial instruments business operators		19,032	20,550	23,804	2.80	+15.8
	Money lenders		45,684	63,954	88,282	10.39	+38.0
	Funds transfer service providers		20,271	29,232	39,122	4.60	+33.8
	Cryptoassets exchange service providers		16,550	19,344	22,667	2.67	+17.2
	Commodity derivatives business operators		318	846	428	0.05	-49.4
	Currency exchange operators		430	655	617	0.07	-5.8
	Electronic monetary claim recording institutions		0	14	3	0.00	-78.6
	Other (Note 3)		51	19	20	0.00	+5.3
Financial leasing operators			71	214	141	0.02	-34.1
Credit card operators			41,106	45,674	57,978	6.82	+26.9
Real estate brokers			11	18	25	0.00	+38.9
Dealers in precious metals and stones			124	138	223	0.03	+61.6
Postal receiving service providers			1	30	35	0.00	+16.7
Telephone receiving service providers			0	0	0	-	-
Telephone forwarding service providers			1	17	5	0.00	-70.6
Other (Note 4)			-	-	14	0.00	-
Total			583,317	707,929	849,861	100.00	+20.0

Note 1: Banks include the annual number of notifications for city banks, regional banks, second-tier regional banks, trust banks, and similar institutions.
2: Norinchukin banks, etc. include the annual number of notifications that is recorded for the Norinchukin Bank, agricultural cooperatives, the Credit Agricultural Cooperative Federation, fisheries cooperatives, and the Fisheries Cooperative Federation.
3: Other includes the annual number of notifications for mutual aid companies, trust companies, and similar institutions.
4: Other includes the annual number of notifications for judicial scriveners and similar entities.

(2) Examples of STR Utilization

The National Public Safety Commission and National Police Agency collect, organize and analyze the STRs and provide investigative organizations other than the prefectural police[*1] as well with those that are considered to be useful for investigating ML offences or their predicate offences to enable the organizations to use them for clarification of the Actual Status and investigations into tax offences (see Tables 46 and 47).

In addition, the number of STRs utilized in investigations and other activities conducted by prefectural police and related authorities in 2024 was 629,135 (see Table 48).

Table 46: Number of Reports Provided to Investigating Authorities and Oher Authorities

	2022	2023	2024
Number of information provide related to STRs (cases)	581,252	685,330	815,318
Number of analytical results provided (cases)	15,990	21,730	26,871

Table 47: Flow of Information on Suspicious Transactions

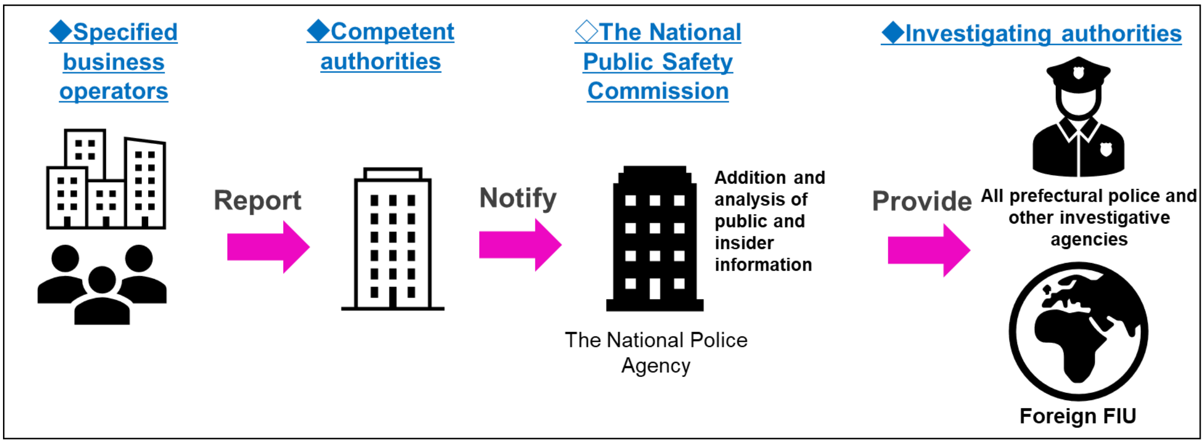


Table 48: Number of Information on Suspicious Transactions Utilized in Investigations and Other Activities

	2022	2023	2024
Number of Information on Suspicious Transactions Utilized in Investigations and Other Activities	373,849	496,093	629,135

Information on suspicious transactions that has been reported is effectively utilized in investigations of ML offences and their predicate offences. Examples of cases where prefectural police or other investigating authorities made arrests based on information on suspicious transactions, as well as cases where such information was utilized in investigations, are as follows:

[*1] Meaning the prosecutors and other authorities set forth in Article 13, paragraph (1) of the Act on Prevention of Transfer of Criminal Proceeds.

(i) Examples of Cleared Cases Detected through STRs by the Prefectural Police[*1*2]

(A) Cases of Violating the Act on Punishment of Organized Crimes (Concealment of Criminal Proceeds)

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	● Large amounts are suddenly deposited from numerous unrelated individuals, followed by transfers to multiple individuals and cash withdrawals from ATMs ● Frequent transfers to multiple unrelated individuals or legal persons ● Cash deposits of unknown origin are made frequently over a short period, followed by ATM cash withdrawals; amounts are high and deviate from previous transaction patterns
Investigation results	It was confirmed that the account holder was involved in withdrawals of the losses from an online and telephone fraud case, and the individual was subsequently arrested.

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	● In addition to having numerous transactions with multiple legal persons, substantial amounts are deposited from an unspecified large number of individuals ● After raising ATM withdrawal and transfer limits to the maximum, all deposited funds are either withdrawn in cash from ATMs or transferred to accounts in the account holder's name at other banks
Investigation results	The account was used in an online and telephone fraud case, and it was confirmed that the account holder also carried out subsequent fund transfers. The individual was subsequently arrested.

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of a corporation
Reason for report	● Cash withdrawals from ATMs within 60 minutes after receiving multiple transfers ● Upon receiving a request to raise the cash card withdrawal limit, the corporate representative was interviewed but could not provide a clear explanation of the purpose of the limit increase, exhibiting unnatural behavior such as consulting a third party via mobile phone while responding ● Suspicious transactions in which the full amount of multiple large transfers was withdrawn from ATMs each time. When interviewed, the corporate representative exhibited unnatural behavior, such as presenting unsigned contracts as documents to justify the transactions
Investigation results	It was confirmed that the account was used in investment fraud via social media case, and that the corporate representatives submitted forged contracts to make misappropriated funds appear legitimate while receiving the proceeds of the crime. The corporate representatives were subsequently arrested.

(B) Fraud cases

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	● After receiving large incoming transfers, funds are either transferred to other accounts or withdrawn in cash, which is unusual compared to typical transactions ● Large transfers are received from a corporate entity, and funds are withdrawn in cash at the teller. When asked for the reason for the cash withdrawals, the customer provided only vague explanations, stating it was an "unspecified time constraint". ● There are suspicious circumstances, such as business funds being transferred through a personal account and the transaction amounts being disproportionately high for the account holder's age.

[*1] There are cases where the report content is not directly related to the charges in the cleared case.

[*2] In the description of the reason for report, a number is assigned indicating the account type.

Investigation results	It was confirmed that the account holder was one of the ringleaders of an investment fraud via social media case, and the individuals were subsequently arrested.

Business type of the reporter	Deposit-taking institution, Cryptoassets exchange service providers
Reported account	Account in the name of Japanese
Reason for report	<Deposit-taking institution> ● A large deposit was suddenly made into an account that had no transactions for more than six months, followed by a full cash withdrawal at a remote ATM on the same day ● Deposits and withdrawals from the account are inconsistent with the declared purpose of the account (for living expenses), indicating unusual activity <Cryptoassets exchange service providers> ● After receiving large deposits, funds are immediately converted into cryptoassets and transferred multiple times
Investigation results	It was confirmed that the account holder was fraudulently receiving government benefits, and the individual was subsequently arrested.

Business type of the reporter	Deposit-taking institution, Insurance companies, Money lenders, Cryptoassets exchange service providers, Financial instruments business operators
Reported account	Account in the name of Japanese
Reason for report	<Deposit-taking institution> ● There are transactions with accounts suspected of being used for criminal activities ● In accounts under the name of individuals reported to have been arrested for unauthorized ATM withdrawals, frequent deposits and multiple transfers from specific persons were observed, indicating suspicious activity <Insurance companies> ● Information provided by a new contract applicant matches information already held by the company regarding Boryokudan or similar entities <Money lenders> ● There is a suspicion that a new contract applicant is a Boryokudan gangster <Cryptoassets exchange service providers and Financial instruments business operators> ● It was confirmed through media reports that a new account applicant had been arrested, and the account opening was refused
Investigation results	It was confirmed that the account holder concealed their status as a Boryokudan gangster, concluded a service contract, and obtained unlawful financial benefits, and the individual was subsequently arrested.

Business type of the reporter	Deposit-taking institution, Cryptoassets exchange service providers
Reported account	Accounts in the name of Japanese and accounts in the names of their relatives
Reason for report	<Deposit-taking institution> ● A large number of deposits from multiple legal persons and individuals were suddenly made into an account that had been inactive for a certain period ● Multiple deposits, including from legal persons, were received, followed by transfers to numerous accounts via online banking or cash withdrawals from ATMs ● Login information in a foreign language, different from usual, was detected in the bank's app, suggesting suspicious activity possibly to verify the functionality of an account intended for transfer <Cryptoassets exchange service providers> ● A report was received from another financial institution indicating that the account in question is being used for fraudulent transactions
Investigation results	It was confirmed that the account holder opened the account for the purpose of allowing third parties to use it and had transferred multiple accounts to such third parties for consideration, and the account holder was subsequently arrested.

(C) Extortion cases

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	● Large deposits and cash withdrawals from ATMs are conducted frequently within a short period ● Multiple large deposits and transfers occur between the account and unrelated individuals

	as well as public racing organizations. In addition, there are substantial cash deposits and withdrawals of unknown origin, which are not consistent with the declared purpose of the account, lacking validity or reasonableness ● The account received transfers from individuals suspected of being Boryokudan gangsters. Multiple transactions with different individuals and frequent cash deposits and withdrawals at ATMs were observed, indicating the possibility that it is a collection account
Investigation results	It was confirmed that the account holder had extorted cash under the pretext of loan repayments, and the individual was subsequently arrested.

(D) Gambling offences (online casino)

Business type of the reporter	Deposit-taking institution, Cryptoassets exchange service providers
Reported account	Account in the name of Japanese
Reason for report	<Deposit-taking institution> ● Determined to be an online casino user based on the IP address and the counterparty's account ● Usage of the bank app was observed from the same IP address as another account with a different account holder and address, raising suspicion of third-party use of the account <Cryptoassets exchange service providers> ● Within a short period, there were frequent receipts of cryptoassets and cash deposits. The cryptoassets were traded, followed by cash withdrawals to the registered account and transfers of cryptoassets to external addresses under the same owner. A portion of the received cryptoassets was transferred to external addresses without being traded even once, indicating unusual activity
Investigation results	It was confirmed that the account holder had engaged in gambling through an online casino, and the individual was subsequently arrested.

(E) Case of Property Losses and Other Acts for the Purpose of Obstructing Compulsory Execution, and Falsification and Use of Original Electronic Notarized Document

Business type of the reporter	Deposit-taking institution
Reported account	1. Account in the name of Japanese, 2.Account in the name of a corporation
Reason for report	● Unusual deposits and withdrawals compared to the transaction history, such as large deposits into personal accounts for the purpose of real estate transactions. [1] ● Frequent transfers observed within a short period, but the total deposits and withdrawals over a certain period are nearly identical. [1] ● After multiple deposits from unrelated legal persons or individuals, funds are transferred to accounts at other banks belonging to persons recognized as relatives. [1] ● There is suspicion that the corporate representative who applied to open a corporate account is a Boryokudan gangster, and the account opening was refused. [2]
Investigation results	It was confirmed that the real estate transactions were conducted for the purpose of obstructing compulsory execution against real estate owned by the account holder, and the individuals were subsequently arrested.

(F) Embezzlement cases

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	● A sudden large deposit was made, which is unusual given the account holder's attribute and the declared purpose of the account (living expenses for a student) ● Deposits from unrelated legal persons and cash of unknown origin were received, followed by transfers to multiple unrelated individuals or cash withdrawals ● The number of ATM withdrawals deviates from past transaction behavior ● Within a short period, large cash deposits of unknown origin were made via ATMs
Investigation results	It was confirmed that the account holder had embezzled funds from the corporation for which they served as the accountant, and the individual was subsequently arrested.

(G) Violation of the Payment Services Act

Business type of the reporter	Deposit-taking institution, Cryptoassets exchange service providers
Reported account	Account in the name of Japanese
Reason for report	<Deposit-taking institution> ● There were multiple large transfers from abroad. Each time funds were received, they were transferred to a financial institution account of a Cryptoassets exchange service providers. <Cryptoassets exchange service providers> ● Due to the high frequency and large amount of transactions, an inquiry was made to the account holder, revealing that they had been asked by an acquaintance to purchase cryptoassets. The transactions were determined to involve the use of third-party funds ● In an account that had been inactive for a long period, deposits exceeding the declared assets were suddenly made within a short period. After purchasing cryptoassets, the funds were transferred to external addresses within a short time
Investigation results	It was confirmed that the account holder had engaged in cryptoassets exchange service business without registration, and the individual was subsequently arrested.

(H) Violation of the Immigration Control and Refugee Recognition Act (encouraging illegal employment)

Business type of the reporter	Funds transfer service providers
Reported account	Multiple accounts in the names of foreigners
Reason for report	● During verification at the time of transaction, when prompted to update the residence card, a forged card was submitted ● The address on the identification document presented differed from the registered address, raising suspicion of forgery. Additional documents were requested but not provided
Investigation results	It was confirmed that multiple foreigners (with illegal overstay) reported in notifications were employed, and the employers were subsequently arrested.

(I) Violation of the Act on Securing the Proper Operation of Worker Dispatching Businesses and Protecting Dispatched Workers[*1]

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	● Funds received from individuals believed to be affiliated with Boryokudan were transferred to multiple unrelated individuals
Investigation results	It was confirmed that associates of the account holder used the account to operate a worker dispatching business without authorization, and the individuals were subsequently arrested.

(J) Violation of the FEFTA

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of a corporation
Reason for report	● Multiple large international transfers from countries that the bank has assessed as high-risk were made ● The account holder’s business activities (household goods export) are inconsistent with the transfer purpose of the counterparties (payment for vehicles), and there are suspicious transactions involving round numbers ● Transfers received from other banks were immediately withdrawn in cash, with withdrawals accounting for over 90% of the account balance
Investigation results	It was confirmed that the representative of the corporation holding the account had exported vehicles abroad without authorization, and the individual was subsequently arrested.

[*1] Act No. 88 of 1985

(K) Violation of the Anti-Nuisance Ordinance (Solicitation of Customers)

Business type of the reporter	Deposit-taking institution
Reported account	1. Account in the name of Japanese, 2. Account in the name of a corporation
Reason for report	● Large transfers were received from individuals identified as Boryokudan gangsters [1] ● There were large deposit and withdrawal transactions, with the total deposits and withdrawals over a certain period being nearly equal. Based on known information and the account holder's attribute, the purpose of the transactions is considered suspicious. [1] ● There were large transfers and inter-account transfers. In addition, funds from recent cash deposits were used to make transfers abroad. [2] ● Large transfers were received from a corporate account with the same name opened at another bank, followed by cash withdrawals from ATMs. [2]
Investigation results	It was confirmed that the account holder, who operates a free information desk for sex-related businesses, had instructed employees to habitually solicit customers to such businesses, and the individuals were subsequently arrested.

(ii) Examples of Cases in Which Investigating Authorities Other than the Prefectural Police Utilized STRs

Examples of cases in which investigative organizations other than the prefectural police utilized STRs for investigation and recent crime cases and trends reported by each investigative organization*1 are as follows:

(A) Public Prosecutors Office

Case name	Fraud case, theft case
Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	● There were transfers into the account that bore no reasonable relation to the account holder's occupation ● All deposits to the account originated from multiple specific individuals and occurred frequently and irregularly ● Funds deposited into the account were transferred to multiple individuals or withdrawn in cash on the same day, resulting in minimal account balances for most periods

[Recent Crime Cases and Trends Reported by the Public Prosecutors Office]

[Possibility of Corporate Acquisitions Being Misused for ML]

- In many cases involving illicit fund transfers, corporate bank accounts are frequently used as initial or subsequent destination accounts.
- Many of these accounts are in the names of companies with no operational activity and were transferred as part of corporate acquisitions.

(B) National Tax Agency

Case name	Cases of violation of Corporation Tax Act/Consumption Tax Act/Income Tax Act
Business type of the reporter	Deposit-taking institution
Reported account	1. Account in the name of Japanese, 2. Account in the name of a corporation
Reason for report	● Following large deposits from a corporation, substantial cash withdrawals were made at the teller. When the account holder was asked about the purpose of the withdrawals, no detailed explanation was provided. [1] ● There were frequent large ATM deposits and transfers to multiple accounts in the names of foreigners. [1] ● An account frequently received deposits from numerous unrelated individuals. Reviewing ATM footage revealed that a third party used the account. [1] ● Compared to past transactions, there were unusually large deposits and transfers to both the corporate representative's personal account and corporate accounts with opaque business activities. [2]

*1 Introduced based on information provided by each investigative organization.

[Recent Crime Cases and Trends Reported by National Tax Agency]

- In FY2024, cases were recommended for prosecution including; consumption tax-related cases (e.g., a case where fraudulent refund schemes in which inexpensive watches purchased online were used to create receipts indicating the purchase of high-end watches to falsely record taxable purchases and export tax-exempt sales, or cases where taxable sales of trading cards were omitted from tax returns to evade required consumption tax payments); non-filing cases (e.g., cases where the following taxpayers failed to file income tax returns: an individual received income from the transfer of shares held by corporations this person represented or an individual received usage fees from video streaming service operators); and international cases (e.g., a case where consulting fees related to online sales of pharmaceuticals operated by foreign corporations were retained in foreign bank accounts to avoid income tax).
- Further, socially impactful cases were also recommended for prosecution, including; a case where a professional enabler instructed salaried employees on the fraudulent refund of withholding income tax; cases where a professional enabler who is a Certified Public Tax Accountant arranged entities to serve as recipients of fictitious outsourcing expenses and then aided and abetted their clients in committing tax evasion; cases where a law firm recorded fictitious outsourcing expenses for transactions with no underlying substance through the use of cooperating parties; a case where a talent agency representing high-profile talent had multiple cooperating parties create fake invoices and service contracts, and then recorded fictitious advertising and outsourcing expenses: acase where a medical corporation providing popular traditional medicine treatments for dieting purposes disguised the director's personal purchase of luxury watches as clinical medical supply expenses.
- An analysis of cases subject to prosecution by type of business shows that construction, real estate and staffing agency businesses are being ranked high in the number.
- Most of the illegal funds obtained through tax evasion are retained in the form of cash or bank deposits. There were cases where tax evaders have spent substantial amount of illegal funds on the purchase of real estate, purchase of luxury vehicles and high-end watches, investments in securities, purchase of cryptoassets, gambling on horse racing and foreign casinos, and entertainment and leisure expenses such as dining and drinking at high-end clubs.

(C) Japan Customs

Case name	Cases of smuggling of illegal drugs
Business type of the reporter	Deposit-taking institution, Cryptoassets exchange service providers
Reported account	1. Account in the name of Japanese, 2. Account in the name of foreigner, 3. Account in the name of a corporation
Reason for report	<Deposit-taking institution> ● Frequent transfer transactions occurred over a short period, with deposit and withdrawal amounts nearly equal over a given period. [2] ● Access was detected from locations far from the account holder's residence, both domestic and overseas, based on IP addresses. [2] ● During customer due diligence, the account holder was observed communicating with someone while wearing a single earphone and avoided answering questions, displaying suspicious behavior. [2] ● The personal identification number card presented at account opening had unusual font characteristics, raising suspicion of forgery. [1] ● Large remittances from abroad were received and immediately transferred out. The business background of the remitter was unclear, and the transaction amounts were excessive compared to past transactions. [3]

	<Cryptoassets exchange service providers> ● When the transaction amount exceeded the reported income, a review was conducted, but the account holder did not comply with requests to submit documentation verifying the source of funds and their identity. [1]

[Recent Crime Cases and Trends Reported by Japan Customs]

- In 2024, the total number of illicit drug seizures by customs nationwide was 1,020 cases, a 24% increase compared to the previous year. The total quantity seized amounted to approximately 2,579 kilograms, a 6% decrease compared to the previous year. Although the quantity seized had reached around 3,339 kilograms in 2019, it subsequently remained below 2,000 kilograms. In 2023, it again exceeded 2,000 kilograms, reaching approximately 2,741 kilograms. In 2024, the seized quantity was about 2,579 kilograms, surpassing 2,000 kilograms for the second consecutive year for the first time.
  This increase is attributed to several factors, which are large-scale seizures involving maritime and air cargo, the consistently high volume of methamphetamine seized, and significant increases in the quantities of cannabis and other narcotics such as heroin, cocaine, and MDMA.
- Gold smuggling is considered to be conducted with the aim of earning a profit equivalent to the amount of consumption tax by selling gold bullion brought into Japan without declaring or paying consumption tax to domestic gold buyers (gold buying stores). Due to efforts including raised penal provision in 2018, the number of gold smuggling cases detected has decreased significantly. However, due to a rapid recovery in inbound tourism and rising gold prices, the number of gold smuggling cases detected and seized quantity have sharply increased. In 2024, customs nationwide reported 493 gold bullion smuggling cases, which is approximately 2.3 times the previous year, with a total quantity seized of about 1,218 kilograms, roughly four times the previous year.

(D) Narcotics Control Department, Regional Bureaus of Health and Welfare, Ministry of Health, Labour and Welfare

Case name	Illicit drug trafficking case
Business type of the reporter	Deposit-taking institutions, Financial instruments business operators, Funds transfer service providers, Cryptoassets exchange service providers
Reported account	1. Account in the name of Japanese, 2. Account in the name of foreigner, 3. Account in the name of a corporation
Reason for report	<Deposit-taking institutions> ● On the account opening day, there were requests for large deposits and cash withdrawals of the same amount. When the reasons were confirmed, they differed from the stated purpose of opening the account. [1] ● Transactions occurred that deviated from past transaction behavior. These included transfers to corporations, including those whose applications to open a corporate account with the bank were rejected, and multiple individuals. [3] ● Suspicious activity was detected via the IP address. Although the account holder resides in Japan, there were accesses from foreign countries and from cities far from the registered address. [2] ● There were frequent cash withdrawals from ATMs over a short period. [2] <Financial instruments business operators> ● Multiple applications to open accounts were submitted using common information*1 by different customers, leading to the determination that the accounts were likely being used for name-lending purposes. [1] <Funds transfer service providers> ● An application to open an account was submitted using an identity document suspected to be a forged license. [1] <Cryptoassets exchange service providers> ● Frequent night-time deposits and withdrawals were made over a short period, and the registered phone number differed from the SMS authentication number. [1] ● Changes to the email address and authentication method were made prior to deposits, which is a behavior frequently observed in fraudulent transactions. [1]

*1 Examples include email addresses that follow identifiable patterns, such as “four alphabetic characters + five digits + domain name” or “part of a name + numbers + domain name.”

[Recent Criminal Cases and Trends Reported by Narcotics Control Department, Regional Bureaus of Health and Welfare, Ministry of Health, Labour and Welfare]

- There were cases where drug purchase payments were made using electronic gift cards, which were then sold to buyback dealer to be converted into cash
- Criminal proceeds obtained from drug trafficking and related offences were converted into cryptoassets for which no exchange exists in Japan.
- When having customers transfer payments for illicit drugs, some used fictitious names such as "Hensai", which means repayment of a debt, to disguise the transfers as if legitimate.
- Vehicles purchased with criminal proceeds from drug smuggling and trafficking were exported abroad and sold for cash there.
- In drug trafficking cases conducted via social media, nominee accounts are still frequently used to receive payments.
- In cases where individuals sell products to each other via social media, some exploit payment services to traffic illicit drugs; in certain cases, some payment service providers refuse to disclose registered information linked to electronic money accounts creating a risk of ML.
- To receive payment for illicit drugs, some traffickers used internet auction sites to post fictitious items and have buyers "purchase" them, thereby disguising the transaction as legitimate, and received payment in the form of site-usable points.

(E) Japan Coast Guard

Case name	Illegal Poaching Case Involving Specified Aquatic Animals and Plants*[1]
Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	● There were frequent transfers and incoming remittances involving individuals of unknown relationship, including persons believed to be affiliated with Boryokudan. Following the deposits, cash withdrawals of the same amount were made at ATMs located far from the account holder's residence. ● Deposits were made using a cash card, while withdrawals were made using a passbook in different regions. Transactions were repeatedly conducted in round amounts with no amounts under 1,000 yen, indicating suspicious activity.

[Recent Crime Cases and Trends Reported by the Japan Coast Guard]

- There are various forms of organized poaching observed, such as organized poaching committed by a group in charge of hunting and capturing in collaboration with a buyer, or poaching which involves Boryokudan, in order to use fish that can be sold at higher prices as a source of funds. Particularly, in recent years, there have been cases of poachers changing their sales channels, such as selling directly to fishery companies rather than through markets, thereby concealing the distribution of poached products, and cases of poached products being distributed being disguised as legitimate products.

*[1] Abalone, sea cucumbers, and glass eels are designated as Class I Specified Aquatic Animals and Plants under the Act on Ensuring the Proper Domestic Distribution and Importation of Specified Aquatic Animals and Plants (Act No. 79 of 2020).

Section 4. Risk of Transaction Types, Countries/Regions, and Customer Attributes

This section analyzes and evaluates high-risk transaction types, countries/regions, and customer attributes from the perspective of factors that increase the risk and measures to mitigate the risk.

The overview of the evaluation in this section is as follows:

<table>
<tr><th>Risk factors</th><th colspan="3">High-risk transactions</th></tr>
<tr><td>1. Transaction types</td><td colspan="3">Non-face-to-face transactions, cash transactions, cross-border transactions</td></tr>
<tr><td rowspan="2">2. Countries/regions</td><td colspan="2">[Particularly high-risk] Countries/regions against which the implementation of countermeasures are requested by the FATF statements</td><td>North Korea, Iran</td></tr>
<tr><td colspan="2">Countries/regions against which the implementation of enhanced due diligence measures are requested by the FATF statements</td><td>Myanmar</td></tr>
<tr><td rowspan="2">3. Customer Attributes</td><td>Persons who intend to commit ML/TF</td><td colspan="2">Boryokudan</td></tr>
<tr><td>Persons for whom it is difficult to conduct CDD</td><td colspan="2">Non-residents
Foreign Politically Exposed Persons (Foreign PEPs)
Legal persons (Legal persons without transparency of beneficial owners)</td></tr>
</table>

1. Transaction Types

By referring to cleared cases in which foreigners visiting Japan committed ML offences, as well as situations that increase the risks of ML/TF (non-face-to-face transactions, cash-intensive businesses) as described in the FATF's Interpretive Notes to the FATF Recommendations, the following types were identified as transactions that affect the level of risk in transactions: (1) non-face-to-face transactions; (2) cash transactions; and (3) cross-border transactions. Then, they were analyzed and evaluated from the perspective of inherent risks of being misused for ML/TF, typologies, trends of STRs, and measures to mitigate risks.

(1) Non-Face-to-face Transactions

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Online non-face-to-face transactions have been increasing rapidly, driven by advancements in information and communication technologies, diversification of services provided by specified business operators focused on customer convenience.

For example, at deposit-taking institutions, it is possible to conduct financial transactions such as account opening, transfers, and cross-border remittances online, without face-to-face interaction, while financial instruments business operators also provide services such as opening accounts and buying and selling shares online. There are also specified business operators, like Cryptoassets exchange service providers, which provide products and services primarily through non-face-to-face transactions.

Non-face-to-face transactions involve conducting transactions without direct face-to-face interaction with the counterparty, making it difficult to verify the individual's identity through appearance, behavior, or other in-person cues. As a result, there is a relatively higher risk of falsified identification matters or transactions conducted through impersonation, and the accuracy of customer due diligence at the time of the transaction tends to be decreased compared to face-to-face transactions. Furthermore, when verification at the time of transaction is carried out through the mailing of identity verification documents or through eKYC[*1], the authenticity of the documents cannot be assessed through physical characteristics such as feel or texture, unlike in face-to-face verification. This may make it more difficult to detect forged or altered identification documents.

In addition, in a non-face-to-face environment, even if deposit accounts or other accounts are transferred or lent to third parties and transactions are conducted by persons other than the account holders, specified business operators cannot easily identify such situations.

Furthermore, online banking and cryptoasset transactions are characterized by features such as immediacy, where the processing time from instruction to completion is extremely short; irreversibility where transactions are difficult to cancel once completed; and ability to execute multiple transfers repeatedly within a short period of time. Owing to these characteristics, if such transaction methods are misused for ML, funds may be dispersed, transferred, or withdrawn within a very short time, making it difficult for financial institutions and other entities to detect unusual transactions and implement preventive measures to block them.

Non-face-to-face transaction channels such as online banking are vulnerabilities, as user authentication credentials may be obtained by third parties through phishing, malware, or similar means, resulting in unauthorized access.

(B) Typologies

In cases of online and telephone fraud and investment/romance fraud via social media, bank transfers conducted through online banking are commonly used as a method of transferring victim funds. Furthermore, with respect to criminal proceeds generated through online and telephone fraud and similar offences, it has been confirmed that such funds are transferred to fictitious or third-party bank accounts and other accounts. Many of these bank accounts are opened using forged or altered identity verification documents, obtained from others in exchange for payment, or effectively controlled by individuals other than the legitimate account holder. These accounts are widely misused as means for receiving and transferring criminal proceeds.

Major cases where non-face-to-face transactions have been misused for ML are as follows:

[Case 1]
Using illegally obtained online banking login passwords, the offenders impersonated others and transferred money to accounts under the names of fictitious or other parties managed by the offenders in non-face-to-face transactions.

[Case 2]
Using the account information of a cryptoassets exchange service providers that had been illegally obtained, the offenders impersonated others through non-face-to-face transactions and transferred cryptoassets from the cryptoassets wallet linked to the account to a cryptoassets wallet managed by the offenders.

[*1] electronic Know Your Customer. A method that allows identity verification to be completed online.

[Case 3]
A criminal obtained a copy of a resident record by impersonating other person with a stolen health insurance card and opened a bank account by using the copy of the resident record and health insurance card to transfer funds loaned through an online non-face-to-face transaction into an account opened by impersonating other person.

[Case 4]
A criminal applied for multiple purchases of a large quantity of heated electronic cigarettes in a short period through non-face-to-face transaction by using illegally obtained credit card information. After receiving the products, the criminal handed them over to accomplices.

(ii) Trends of STRs

Suspicious indicators related to non-face-to-face transactions include signs of fraudulent acquisition of accounts, unauthorized use by third parties, unusual transfers via online banking, and factors related to users' behavior or background.

The reasons for submitting STRs regarding non-face-to-face transactions that focus on transactions suspected of involving impersonation of fictitious persons or other individuals, or the use of third parties, are as follows:

- Many accounts with different account holders have been opened from the same device (IP address), raising suspicions that the accounts have been opened through impersonation.
- For an account suspected of having forged identity documents during verification at the time of transaction, the registered email address is the same as that of an individual involved in suspicious transactions.
- Immediately after opening the account, the transfer limit was raised, and after making multiple deposits via ATM, the money was transferred to the securities company's account. In addition, upon checking the images from the ATM security camera, it was found that a person other than the person in the photo on the identification document was operating the ATM, which revealed that a third party had used the ATM.
- There is suspicion of third-party use, as the account holder is Japanese but the language setting of the browser used to access the account is in a foreign language, and the IP address location shows a distant location that differs from the registered address.
- There have been many transfer deposits to the accounts that have not had any transactions since the account was opened, with the name of the sender changed to "numbers + individual name," and cash has been withdrawn or transferred to corporate accounts using ATMs.
- After multiple transfers were made from a corporate account to a personal account, the name of the person sending the transfer was changed to the name of a major e-commerce site and the money was then transferred to a funds transfer service provider from the account in the name of such individual, making the transaction appear unnatural.
- After cash was deposited into a funds transfer services account via ATM, it was immediately withdrawn from a distant ATM, raising suspicion that the account was used by a third party.

(iii) Measures to Mitigate Risks

(A) Statutory measures

○ Act on Prevention of Transfer of Criminal Proceeds and the Ordinance of the Act on the Prevention of Transfer of Criminal Proceeds

Under the Act on Prevention of Transfer of Criminal Proceeds and the Ordinance of the Act on the Prevention of Transfer of Criminal Proceeds, in addition to verifying identification matters by presenting identification documents in person, the following non-face-to-face methods using identification documents are also prescribed:

- A method of receiving image data of a customer's identification document captured using software provided by a specified business operator
- A method of receiving a copy of the customer's identification document and sending transaction-related documents via registered mail or similar means, without forwarding

Unlike face-to-face verification methods, these methods do not allow for physical verification of the texture or quality of identification documents. As a result, there is the issue that such methods may be susceptible to impersonation through forgery or alteration of identification documents.

As statutory measures to address these issues, a partial amendment to the Ordinance of the Act on the Prevention of Transfer of Criminal Proceeds was promulgated in June 2025, which includes the abolition of non-face-to-face identification matters that carry a high risk of impersonation through forgery or alteration of identification documents. Awareness and dissemination of these changes are being promoted ahead of their enforcement in April 2027.

It should be noted that, in recent years, even when verifying identification matters face-to-face, forged or altered identification documents have been misused, posing a significant public security challenge. In light of these circumstances, revisions to the relevant provisions of the Ordinance of the Act on the Prevention of Transfer of Criminal Proceeds are being considered to, in principle, require that face-to-face verification of identification matters involve not only the presentation of identification documents but also the reading of IC chip data.

(B) Measures by business operators

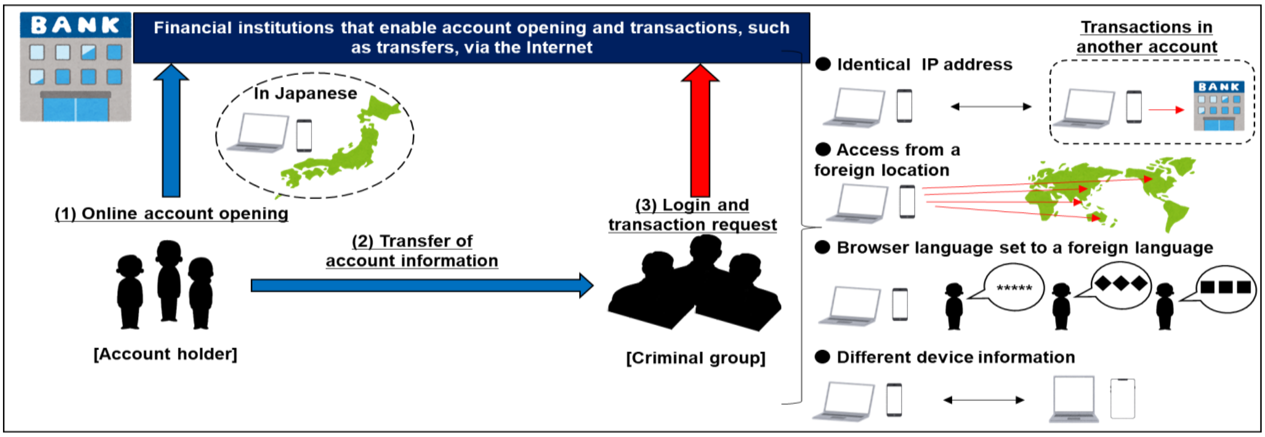
As practical measures to mitigate risks in non-face-to-face transactions, specified business operators conduct ongoing monitoring after the completion of verification at the time of transaction, taking into account the possibility for unauthorized transactions by third parties.

Specific measures include:

- Verifying the consistency of login IP addresses, access locations, browser language settings, and device information
- Confirming customers' registered information such as phone numbers and email addresses
- Conducting 24/7 transaction monitoring
- Detecting changes to registered contact information or transfer limits
- Monitoring transactions with attention to signs such as unusual login frequency or unusual fund movements

If suspicious transactions or other irregularities are detected through such monitoring, appropriate measures such as restricting the use of the account are taken as necessary.

Table 49: Examples of Indicators for Detecting Suspected Unauthorized Transactions by Third Parties in Non-Face-to-Face Transactions



(iv) Assessment of Risks

As non-face-to-face transactions prevent specified business operators from directly observing customers and identification documents, the accuracy of verification at the time of transaction tends to be lower than in face-to-face transactions. Therefore, compared with face-to-face transactions, there is a higher risk that offenders falsify identification matters using forged or altered identity verification documents, or open bank accounts or accounts using fictitious names or by impersonating another person. In addition, even after verification procedures has been completed, the risk that transactions may be conducted by third party other than the account holder is higher than in face-to-face transactions.

Furthermore, in transactions such as online banking and cryptoasset trading, transfer of funds can be completed within a very short period of time, and once completed, transactions are difficult to cancel due to the contractual terms and technical specifications of online banking. As a result, it is difficult for financial institutions and other entities to detect unusual transactions and block them in order to prevent the transfer of criminal proceeds.

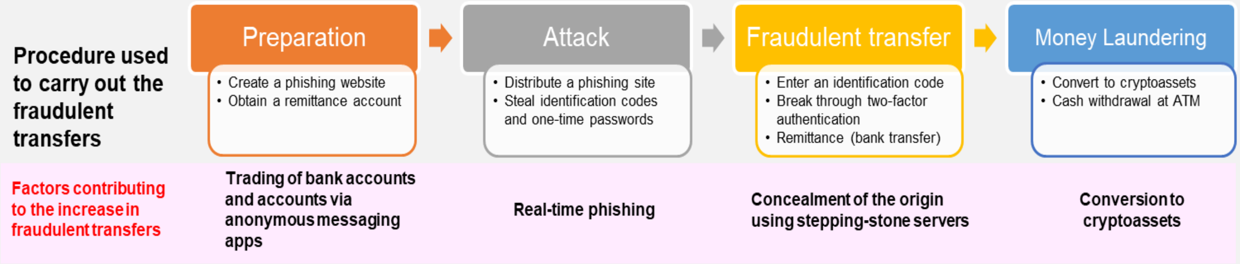
Actually, there are numerous cases where bank accounts opened through non-face-to-face transactions have been misused for ML by individuals impersonating the account holders or by third parties to whom the accounts had been transferred. Considering these facts, it is assessed that non-face-to-face transactions present a high risk of being misused for ML/TF and are of high risk transaction.

[Topic] Fraudulent Transfers, Online and Telephone Fraud, Investment/Romance Frauds via Social Media Using Online Banking

Online banking is widely used by both individuals and legal persons due to its convenience, allowing financial transactions at any time. On the other hand, examples of misuse of online banking vulnerabilities include fraudulent transfers using online banking through phishing and other means, as well as cases where losses of online and telephone fraud or investment/romance fraud via social media are instructed to remitted via online banking. Furthermore, the criminal proceeds from these offences have subsequently been observed to be subject to ML.

1. Unauthorized Transfers Involving Online Banking[*1]

In 2024, losses from online banking fraud have remained at a high level. Fraudulent transfers involving online banking generally proceed through four stages: (i) preparation, (ii) attack, (iii) fraudulent transfer, and (iv) money laundering. According to the analysis by the Cyber Special Investigation Division of the Kanto Regional Police Bureau, changes in modus operandi have been observed at each stage in recent years, which are considered to be a contributing factor to the increase in the number of incidents.



1	Preparation stage	Bank accounts used to receive fraudulent transfers and accounts at cryptoasset exchanges for converting funds into cryptoassets are being illegally bought and sold via highly anonymous messaging apps, making them easily accessible.
2	Attack stage	Since around 2019, methods of bypassing two-factor authentication through real-time phishing[*2] have been widespread.
3	Fraudulent transfer stage	There have been numerous confirmed cases where perpetrators conceal (anonymize) the origin of their communications by misusing general household internet connections or third parties' mobile communications as stepping stones, while at the same time disguising their access as legitimate logins originating from general households. For example, there have also been confirmed cases where IoT devices used to watch television programs broadcast overseas or videos streamed over the internet were infected with malware and then exploited as stepping stones.
4	Money laundering and cashing stage	Instead of the conventional method in which so-called "Dashiko" (cash withdrawal operative) withdraw cash from ATMs, money laundering through conversion into cryptoassets has become the mainstream approach. Criminals obtain bank accounts used to receive fraudulent transfers, as well as accounts for converting funds into cryptoassets, through buying and selling, and launder criminal proceeds not only by withdrawing cash from ATMs but also by converting the funds into cryptoassets.

2. Actual Use of Online Banking in Online and Telephone Fraud and Investment/Romance Fraud via Social Media [*3]

(1) Actual Use of Online Banking

A survey was conducted on the actual use of online banking in online and telephone fraud and investment/romance fraud via social media, in which both the number of recognized cases and the amount of losses have been increasing, and the findings were as follows.

○ Online and Telephone Fraud

A survey was conducted regarding transfer-type fraud cases in 2024 involving losses of 5 million yen or more (1,673 recognized cases, with total amount of losses of 30.77 billion yen). The summary of the results is as follows:

- The use of online banking accounted for approximately 60% of the number of recognized cases and about 70% of the total amount of losses.
- Both the number of recognized cases and the amount of losses involving the use of online banking are on an upward trend.

[*1] See "The threat situation surrounding cyberspace in 2024" (March 2025, Cyber Affairs Bureau, National Police Agency).

[*2] The suspect immediately enters the information that the user entered into the phishing site into the legitimate site, and then has the user enter the one-time password for two-step authentication that is sent to the user into the phishing site, thereby attempting unauthorized access.

[*3] See the materials posted on the National Police Agency website (https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/sagi_keihatsu2024.pdf).

- Approximately 70% involved accounts for which victims had set up online banking functions prior to becoming a victim.
- There were confirmed cases where victims, under the suspect's instructions, opened online banking accounts or additionally enabled online banking functions, as well as cases where suspects opened such accounts in the victims' names.

Table 50: Trends in Losses from Transfers via Online Banking in Online and Telephone Fraud

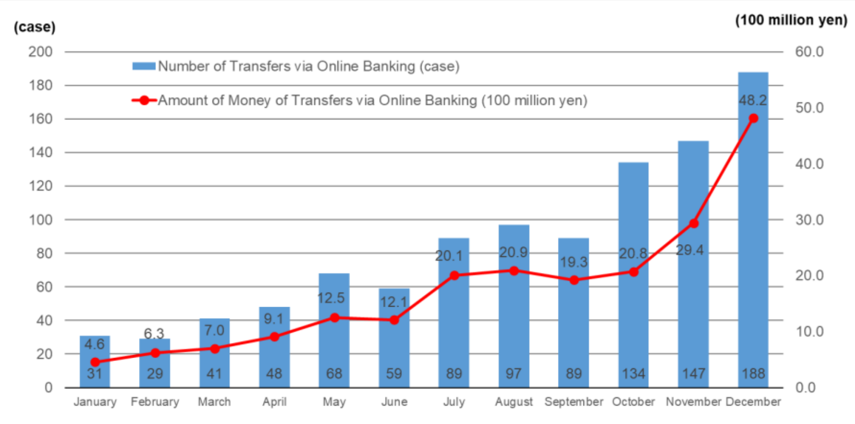


Table 51: Status of Online Banking Setup by Modus Operandi of Online and Telephone Fraud (Number of Recognized Cases)

	"It's me" fraud	Fictitious fee request fraud	Refund fraud	Loan guarantee fee fraud	Financial instruments fraud	Gambling	Dating service scam	Other	Total
Account Opening (the victim, under the instructions of the suspect, opens an account with online banking functionality)	123	9	0	0	4	0	0	1	137
New Account Opening (the suspect opens an account with online banking functionality in the victim's name)	20	1	0	0	0	0	0	1	22
Additional Setup for Existing Account (the victim sets up online banking under the suspect's instructions)	87	10	5	0	1	0	0	2	105
Additional Setup for Existing Account (the suspect obtains account information from the victim and sets up online banking)	10	0	0	0	0	0	0	0	10
Use of Existing Account (online banking is already set up by the victim prior to the fraud)	560	92	45	2	8	4	10	16	737
Uncertain	5	4	0	0	0	0	0	0	9
Total	805	116	50	2	13	4	10	20	1,020

○ Investment/Romance Fraud via Social Media

In 2024, a survey was conducted on transfer-type fraud cases (8,349 recognized cases, total amount of losses of 107.43 billion yen), which revealed that the use of online banking accounted for approximately 60% of the recognized cases and about 70% of the total amount of losses.

Online and telephone fraud and investment/romance fraud via social media are believed to be largely carried out as revenue-generating activities by Anonymous and fluid criminal groups. As illustrated in specific cases*1 included in this NRA-FUR, in the context of online and telephone fraud, criminal proceeds are laundered not only through cash withdrawals from ATMs within Japan, but also via fund transfers through multiple bank accounts, conversion into cryptoassets, foreign remittances, and methods such as cash couriers.

(2) Measures to Mitigate Risks by Specified Business Operators

The fact that online banking transaction limits can be changed without face-to-face manner, together with transfers of amount close to the daily limit over consecutive days, has contributed to an increase in the amounts of losses. Therefore, it is important to implement measures such as verification and warnings when applying for online banking, appropriately setting initial transaction limits, and providing confirmation and warnings to users when raising limits. Measures aimed at preventing victimization are being considered.

*1 Details of the cases are described in this NRA-FUR under "Chapter 3: Analysis of Money Laundering Cases," Section 1: Offenders, Subsection (1) Anonymous and Fluid Criminal Groups, Part (c) Modus Operandi of Money Laundering Offences Involving Anonymous and Fluid Criminal Groups.

(2) Cash Transactions

(i) Factors that Increase Risks

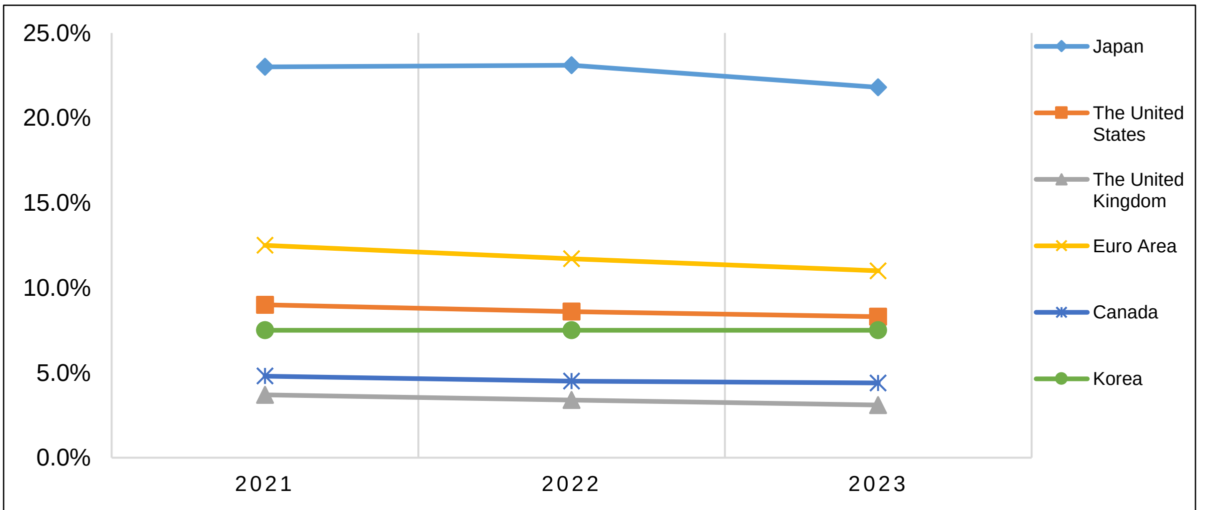
(A) Inherent Risks of Being Misused for ML/TF

Unlike fund transfers that enable funds to be moved quickly to remote locations, cash transactions require a certain amount of time because they involve the physical movement of cash. However, cash transactions are highly anonymous, and if such transactions are not recorded by financial institutions or other entities, the flow of funds can be difficult for law enforcement authorities, including the police, to trace. Additionally, cash can be easily withdrawn from widely available ATMs and readily converted into other types of assets. These characteristics can make cash susceptible to be misused for ML/TF.

In Japan, cash continues to be widely used as one of the primary means of payment, and the ratio of cash in circulation to nominal GDP is relatively high compared to other countries (see Table 52). Meanwhile, the "Follow-up on the Growth Strategy" (Cabinet decision of June 21, 2019) set a goal of increasing the cashless payment ratio to around 40% by June 2025. As a result of efforts to promote this target, the cashless payment ratio has steadily increased, reaching 42.8% in 2024 (see Table 53).

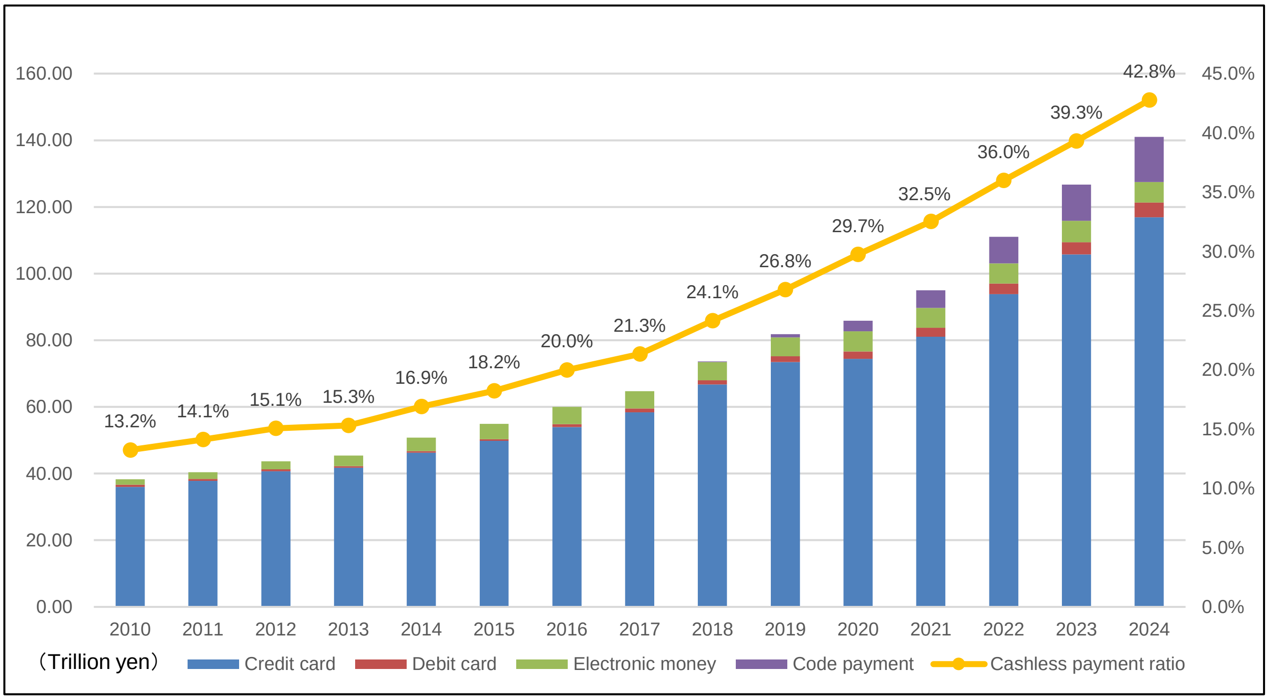
In this context, financial institutions are seeing a decrease in opportunities for face-to-face transaction due to branch consolidation and operational efficiency measures, and some cash transactions previously conducted face-to-face are now being carried out through ATMs. In ATM-based transactions, it is more difficult to ascertain the purpose and background of the transactions compared with face-to-face transactions. In addition, there is variation in the frequency and timing of cash transaction monitoring by specified business operators.

Table 52: Ratio of Cash Distribution Balance for Different Countries in Nominal GDP



Source: BIS Statistics Explorer

Table 53: Trends in the Cashless Payment Ratio



(B) Typologies

In cases where cash transactions were misused, offenders took advantage of the anonymity of cash to transfer criminal proceeds in the form of cash. Other methods observed include withdrawals and deposits via ATMs, as well as purchases of assets using cash and the conversions of assets into cash.

The major examples of cash transactions being misused for ML are as follows:

[Case 1]
An offender sold stolen goods, which were the proceeds of crime from theft, to pawnshops and secondhand dealers by impersonating fictitious people or others, and converted the proceeds into cash.

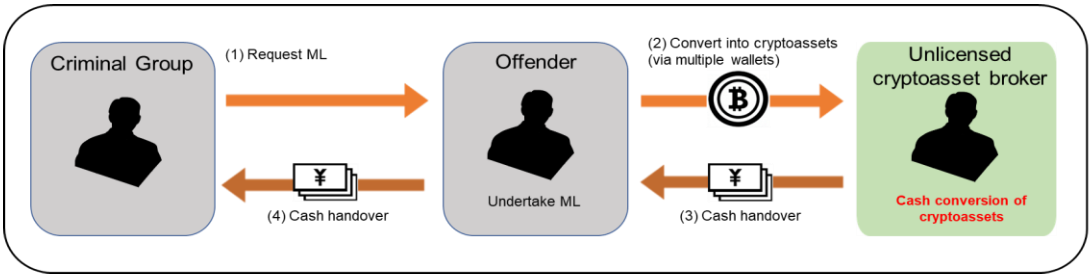
[Case 2]
An offender exchanged the cash, which was the proceeds of crime from robbery, for high-denomination bills at financial institutions and used ATMs to deposit the cash into an accounts in the relative’s name.

[Case 3]
An offender withdrew some of the criminal proceeds obtained from fraud from a corporate account managed by the suspect, and then entered into fixed-term deposits in the name of a relative at financial institutions and deposited the money into the account.

[Case 4]
An offender purchased a car with the cash, which was the proceeds of crime from robbery, and then sold it to a car dealer shortly thereafter, turning it into cash.

In addition, there have been cases where cash derived from criminal proceeds was converted into cryptoassets, transferred through multiple cryptoasset wallets, and then converted back into cash via an unlicensed cryptoasset broker[*1].

Table 54: Illustration of Converting Cryptoassets into Cash via Unlicensed Cryptoasset Broker



Furthermore, as there have been cases where cash derived from criminal proceeds was carried abroad by cash couriers, it is also conceivable that criminal proceeds transferred overseas via foreign remittances or cryptoassets could be converted into cash and brought back into the country.

(ii) Trends of STRs

Suspicious cash transactions are assessed by focusing on multiple indicators, including the transaction amount, frequency or behavioral patterns, the purpose or background of the transaction, and any changes to transaction limits.

In terms of reasons for submitting STRs regarding cash transactions, the following reports focused on transactions utilizing anonymity:

- Consecutive cash transfers on the same day at an ATM (the transfer requester’s name used only the recipient’s surname, and a different phone number was registered to prevent identification of the requester) were detected, and when the images captured by security camera were checked, it was found that the person using the ATM was wearing sunglasses on a rainy day and also a mask, raising suspicion of third-party use.
- It appears that the person deliberately does not withdraw cash over the counter, but repeatedly withdraws the maximum amount allowed from an ATM.
- After raising the maximum withdrawal and transfer limits at ATMs to the maximum, the funds transferred from a personal account at another financial institution are withdrawn in full at an ATM located far from the registered address.
- After receiving a large amount of money from a corporate account, the money was withdrawn from an ATM every day just after midnight.

(iii) Measures to Mitigate Risks

(A) Statutory measures

○ The Act on Prevention of Transfer of Criminal Proceeds and its Enforcement Order

They require specified business operators who operate financial businesses to conduct CDD. This includes conducting verification at the time of transactions as well as preparing and preserving verification records and transaction records when they conduct transactions that accompany the receipt and payment of cash of more than 2 million yen (100,000 yen in the case of transactions that accompany exchange transactions or the writing of a cashier’s check).

○ The Secondhand Goods Business Act (Act No. 108 of 1949) and the Pawnbroker Business Act (Act No. 158

[*1] A party that conducts transactions directly between seller and buyer, setting the price, quantity, and other terms themselves, without going through a stock exchange or other market.

of 1950)

They require the address, name, etc., of the counterparty to be verified at the time of a transaction (with some exemptions for verification under the Secondhand Goods Business Act).

In light of the increasing incidence of metal theft, a revision was made to the Ordinance for Enforcement of the Secondhand Goods Business Act to require business operators, regardless of the transaction amount, to verify the identity of sellers when dealing in certain secondhand items such as outdoor units of air conditioners, electrical wires, and gratings. This revision came into effect in October 2025.

○ The FEFTA and the Foreign Exchange Order (Cabinet Order No. 260 of 1980), and the Customs Act (Act No. 61 of 1954)

As for cash couriers, the FEFTA requires those who export or import the means of payment, such as cash, exceeding the equivalent of 1 million yen (100,000 yen in a case bound for North Korea) to file a notification to the Minister of Finance, and the Customs Act also requires that export or import declarations of goods mentioned above to the Director-General of Customs. Customs authorities work closely with relevant agencies to enhance the collection, analysis, and utilization of information and engage in border control efforts, including introducing currency dogs, to prevent the illicit export or import of cash and other items abroad.

(B) Policy measures

Furthermore, the Japanese government has set targets for the cashless payment ratio in the “Follow-up on the Growth Strategy” (Cabinet Decision on June 21, 2019) and has been promoting the development of cashless environment, based on the “Grand Design and Action Plan for a New Form of Capitalism 2023 Revised Version” and “Follow-up on the Growth Strategy” (Cabinet decision on June 16, 2023). The development of cashless transactions is expected to help prevent ML/TF misusing cash transactions by making opaque cash assets visible and curbing cash circulation.

(C) Measures by Business Operators

Examples of specified business operators’ measures to mitigate the risk are as follows:

- Lowering withdrawal limits at ATMs to prevent elderly victims from falling prey to online and telephone fraud and similar crimes
- For cash deposits and withdrawals that exceed a certain level, verification is conducted at the counter by, for example, issuing a hearing sheet and asking questions to confirm the rationale for using the institution in light of the transaction purpose and the customer’s attributes.
- Refusing cross-border remittance transactions involving cash brought in or deposited into ATMs just before the transaction when there is no rationality for cash transactions.
- Detecting transactions that are high in amount, high in frequency, or involve withdrawals from an ATM located far from the ATM used for deposits, and conducting investigations into the account’s purpose of use, source of funds, and use of funds. If anomalies are detected, submitting STRs and/or conducting enhanced identity verification at the time of transactions as defined in the Act on Prevention of Transfer of Criminal Proceeds, and restricting the use of accounts suspected of being used for crimes.
- Requesting transfer to financial institution accounts instead of conducting cash transactions for payments for jewelry and precious metals exceeding a certain amount.
- Not generally conducting cash transactions for real estate transactions. If a cash transaction is to be conducted, investigating the source of funds and other relevant factors and confirming their reasonableness.

(vi) Assessment of Risks

Cash transactions have high anonymity and characteristics that may hinder the tracing or clarification of the flow of funds. In fact, there have been many cases where money launderers receive criminal proceeds such as funds obtained through online and telephone fraud in cash and transfer them, demonstrating ML through cash transactions. Considering this situation, it is assessed that cash transactions are a type of transaction carrying a high risk of being misused for ML/TF, and therefore are of high risk.

(3) Cross-border Transactions

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Considering its import and export volumes, Japan is occupying an important position in global economy. In addition, it has a highly advanced financial market and conducts a large number of transactions, making it one of the world's leading international financial markets.

Table 55: Statistics on Transactions with Foreign Countries

Item	Amount (yen)
Export value	107,087.9 billion
Import value	112,559.1 billion
Foreign exchange yen settlement amount	6,044.3634 trillion
Annual cross-border transaction value of funds transfer service providers	2,130.5 billion

Note: The export value, import value and foreign exchange yen settlement amount are the results for 2024, and the annual cross-border transaction value of funds transfer service providers is the result for 2023.

Although cross-border transactions are conducted routinely, domestic legal and transaction systems vary from country to country and monitoring and supervision implemented in one country may not be applied in other nations. For these reasons, cross-border transactions have the nature that making it more difficult to track the transfer of funds compared to domestic transactions.

In particular, cross-border exchange transactions are often entrusted based on correspondent agreements[*1] between banks, and such transactions typically passes through a series of remotely located intermediary banks within a short period, which may significantly hinder the tracing of criminal proceeds. In transactions under correspondent agreements, because a correspondent's financial institution may not have a direct relationship with the remittance originator, there is a risk that ML could occur unless the correspondent's institution (the other party to a correspondent contract) develops internal control systems for AML/CFT. For example, if a correspondent's financial institution is a fictitious bank that does not actually do business (what is called a "shell bank"), or if a correspondent's financial institution allows shell banks to use accounts provided by the correspondent, there is a high risk that foreign-exchange transactions could be used for ML/TF.

In addition, some foreign countries/regions allow nominee systems, under which corporate officers or shareholders can be registered under a third party's name. It has been observed that shell companies established in such countries/regions are sometimes misused to conceal criminal proceeds, and routing funds through multiple accounts held by these highly anonymous legal persons increases the risk that the ultimate recipient of the funds becomes opaque.

Furthermore, advances in IT technology have diversified payment methods and ways to transfer funds abroad, making cross-border transactions increasingly complex and heightening vulnerabilities. In addition to traditional cross-border exchange transactions conducted through banks, instant foreign remittance using funds transfer service providers or cryptoassets are now being utilized, which further complicates the identification of the source of funds and the ultimate recipients.

[*1] Contracts for continuous or repeated exchange transactions with exchange transaction business operators located in foreign countries.

(B) Typologies

In cases where cross-border transactions were misused, not only domestic offenders such as Anonymous and fluid criminal groups or crime groups of foreigners in Japan, but also participation of international criminal organizations and the presence of ringleaders located overseas were also recognized.

The modus operandi include:

(1)	Misuse financial institutions in Japan and abroad (e.g., cross-border remittances) while disguising the purpose of sending or receiving funds
(2)	Disguising ML as legal trading (e.g., export or import of goods)
(3)	Provision of domestic and cross-border remittance and payment services without actually moving funds (so-called “underground banking”)
(4)	Use cash couriers
(5)	Misuse of transfer of cryptoassets

(1) In ML cases that misuse financial institutions in Japan and abroad (e.g., through foreign remittances) and involve falsifying the purpose of sending or receiving funds, the following modus operandi have been observed:

- Transfer of criminal proceeds obtained in Japan through online and telephone fraud or investment/romance fraud via social media, as well as wagers related to online casinos
- Receipt of criminal proceeds abroad, such as from BEC*1 schemes

In these cases, the funds are disguised as legitimate in order to conceal the true source and nature of the funds.

Additional characteristics include:

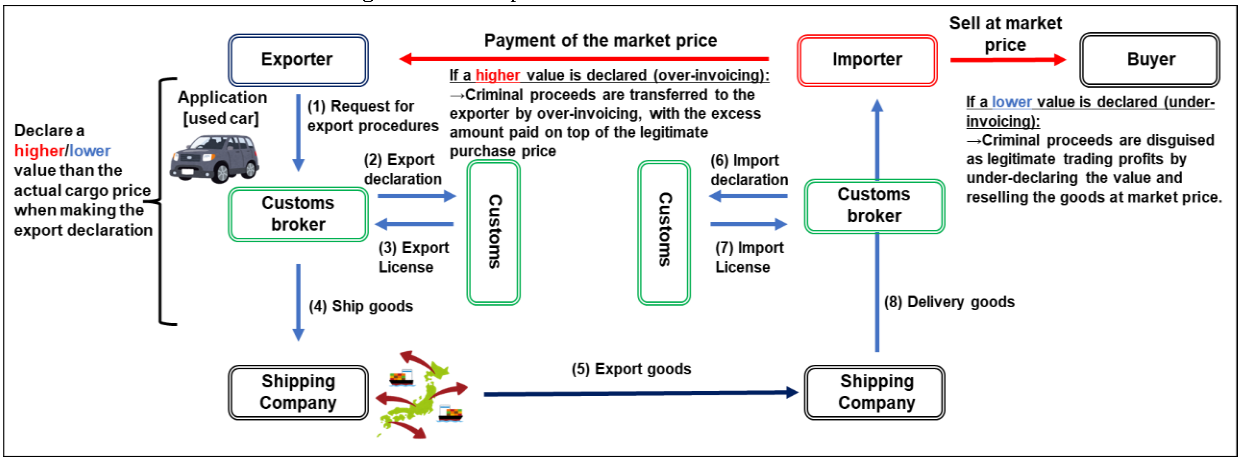
- Transfers being split into smaller amounts per transaction
- The use of fictious service payment (e.g., consulting fees, advertising fees, software usage fees) as the stated purpose of the transfer of receipt of funds
- Different explanations for the purpose of the transfer given by the sender and the recipient.
- Almost all the remitted amount received being withdrawn in cash
- Request from the sender to reverse the transfer at later stage

(2) ML cases disguised as legitimate trade include the following modus operandi:

- When exporting used vehicles, to declaring export values higher or lower than the actual value of the goods so that the difference can be used to transfer criminal proceeds when the payment for the goods is made (see Table 56).
- Exporting goods in high demand overseas (such as automobiles and heavy machinery) under the guise of legitimate trade, selling them overseas for cash, and thereby effectively transferring funds abroad.

*1 Business Email Compromise Refers to business email scams.

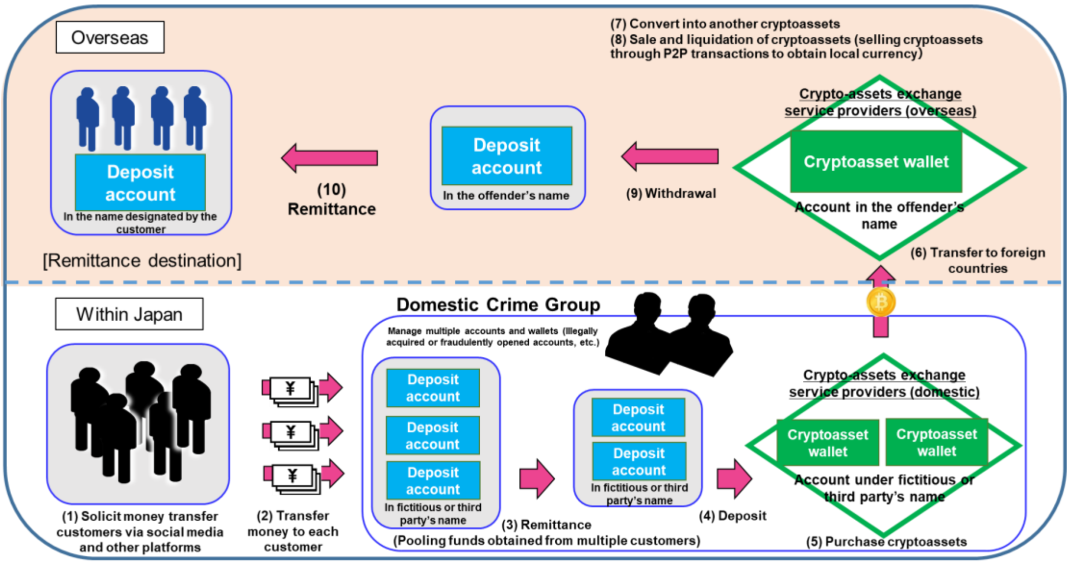
Table 56: Illustration of ML Using Used Car Export



(3) In so-called underground banking cases, in which domestic or cross-border remittances and payments services are provided without actual cross-border movement of funds, the following modus operandi have been observed:

- The operator of an underground bank uses funds deposited by a client into a domestic account to purchase cryptoassets, transfers the cryptoassets to foreign cryptoasset wallets, sells them via P2P[*1] transactions to obtain foreign currency, and then transfers the funds to a foreign bank account specified by the client
- The operator of an underground bank exports goods in high demand overseas under the guise of legitimate trade, sells the goods locally to obtain foreign currency, and then transfers the funds to a foreign bank account designated by the client.

Table 57: Case of Underground Banking Using Cryptoassets



(4) In ML cases involving cash couriers, the following modus operandi have been observed:

- Withdrawing criminal proceeds obtained through online and telephone fraud in cash and having couriers transport them to a foreign country where the ringleaders are located

---

*1 Peer-to-Peer (P2P) transactions, referring to transactions between individuals.

(5) In ML cases misusing transfer of cryptoassets, the following modus operandi have been observed:

- Purchasing cryptoassets with criminal proceeds obtained through fraud, transferring them through multiple cryptoasset wallets, and then selling the cryptoassets to convert them into cash

In addition, in 2024, foreign authorities uncovered foreign bases involved in online and telephone fraud and investment fraud via social media, and 50 individuals were extradited or otherwise brought to Japan and arrested. The countries where the uncovered operation bases were located include Cambodia (8 cases, 28 individuals), the Philippines (4 cases, 14 individuals), Vietnam (2 cases, 6 individuals), and Thailand (2 cases, 2 individuals). It was recognized that criminal proceeds were transferred to ringleaders and others located abroad using modus operandi such as those described above.

ML cases misusing cross-border transactions include the following:

[Case 1]

Criminal proceeds obtained through frauds (such as BEC) carried out in the United States, Europe, and other regions were transferred into bank accounts opened in Japan. The Japanese account holders then explained to the financial institution that the funds were for “office supplies” and submitted false invoice documents to make it appear as if the transfer was a legitimate transaction, before withdrawing the fraudulent proceeds.

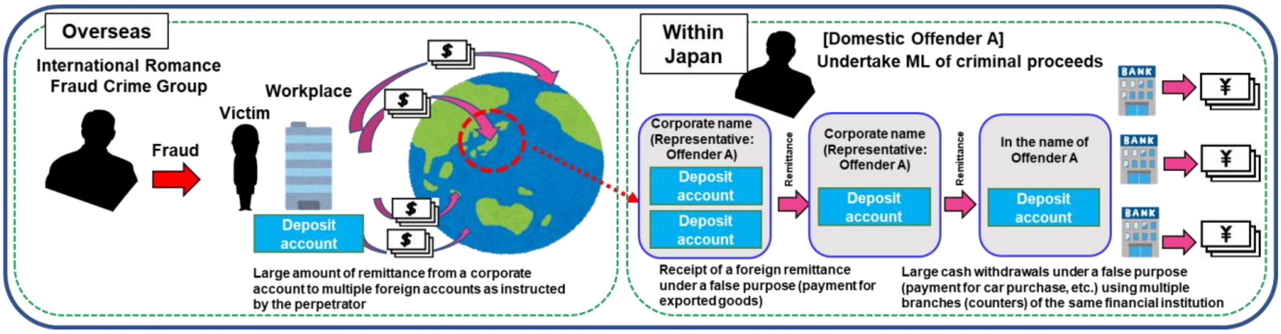
[Case 2]

When transferring the fraudulent proceeds abroad, a false reason for the remittance was entered in the relevant documents, and false invoice documents, purporting to relate to the import of cocoa beans that never actually took place, were submitted as supporting evidence, thereby disguising the transfer as a legitimate commercial transaction, and the funds were sent to an account opened in the suspect’s name at a foreign bank.

[Case 3]

Without being registered as a Type I Financial Instruments Business Operator, the suspect operated an over-the-counter derivatives trading site and caused customers to transfer funds related to their trades, via credit card payments, into an account held in the name of a foreign corporation controlled by the suspect.

Table 58: ML Cases Related to International Fraud



(ii) Notification of STRs

(A) Notification of STRs by Countries/Regions

The number of notifications of STRs related to cross-border remittances from 2022 to 2024 is as follows:

Table 59: Annual Number of Notifications of STRs Related to Cross-border Remittances

Ranking	Destination (origin) countries/regions	2022 (Number of cases)	2023 (Number of cases)	2024 (Number of cases)	Total (Number of cases)	Percentage (%)
1	China	11,286	13,428	16,040	40,754	30.7
2	Hong Kong	3,900	3,355	3,950	11,205	8.4
3	USA	3,866	3,178	3,824	10,868	8.2
4	Vietnam	5,714	2,165	2,345	10,224	7.7
5	Philippines	2,146	2,354	2,008	6,508	4.9
6	Taiwan	1,975	1,616	1,768	5,359	4.0
7	Singapore	1,718	1,383	1,689	4,790	3.6
8	South Korea	1,749	1,398	1,547	4,694	3.5
9	United Kingdom	1,633	1,029	1,241	3,903	2.9
10	United Arab Emirates	709	1,414	1,696	3,819	2.9
11	Thailand	716	784	862	2,362	1.8
12	Russia	917	774	655	2,346	1.8
13	Australia	696	604	635	1,935	1.5
14	Indonesia	599	625	631	1,855	1.4
15	Cambodia	637	733	324	1,694	1.3
16	Ireland	246	411	626	1,283	1.0
17	Canada	444	327	339	1,110	0.8
18	Malaysia	388	378	293	1,059	0.8
19	Turkey	256	291	373	920	0.7
20	Germany	233	217	284	734	0.6
-	Others	4,760	4,984	5,770	15,514	11.7
-	Total	44,588	41,448	46,900	132,936	100.0

The main reasons for the notification of STRs regarding top 10 countries/regions in 2024 were “Large amount of remittances from a country lacking economic rationality,” “Large amount of remittances to a country lacking economic rationality” and “overseas remittance with false information provided,” with the number of cases for each reason as follows:

Table 60: Number of Cases by Reasons for Top Countries/Regions

Large amount of remittances from a country lacking economic rationality		
Ranking	Origin countries/regions	Number of Cases
1	China	13,417
2	Hong Kong	3,001
3	USA	2,336
4	Taiwan	1,395
5	Singapore	1,267
6	South Korea	1,113
7	Vietnam	1,093
8	United Arab Emirates	990
9	United Kingdom	739
10	Philippines	561

Large amount of remittances to a country lacking economic rationality and overseas remittance with false information provided		
Ranking	Destination countries/regions	Number of Cases
1	China	1,220
2	USA	720
3	Hong Kong	456
4	Philippines	360
5	Vietnam	205
6	South Korea	194
7	Singapore	191
8	Taiwan	154
9	United Arab Emirates	153
10	United Kingdom	132

The main reasons for the notification of STRs in 2024 for the top five countries are as follows:

○ China

More than 80% of reports involve “Large amount of remittances from a country lacking economic rationality.” This is followed by “Large amount of remittances to a country lacking economic rationality” and “Overseas remittance with false information provided.” In addition, transfers from accounts in individual names account for over 90% of the reports, particularly high for the category of ‘Large amount of remittances from a country lacking economic rationality.”

○ Hong Kong

The main reasons for the notification of STRs, in order of frequency, are: “Large amount of remittances from a country lacking economic rationality,” Large amount of remittances to a country lacking economic rationality” and “Overseas remittance with false information provided.” In the case of ‘“Overseas remittance with false information provided,” more than 70% of the transfers were made from accounts in corporate names.

○ United States

The main reasons for the notification of STRs, in order of frequency, are: “Large amount of remittances from a country lacking economic rationality,” “Large amount of remittances to a country lacking economic rationality” and “Overseas remittance with false information provided.”

○ Vietnam

The main reasons for the notification of STRs, in order of frequency, are: “Large amount of remittances from a country lacking economic rationality,” “Refusal to provide true beneficiary explanations and materials” and “Large amount of remittances to a country lacking economic rationality.” In addition, following China, the proportion of transfers from accounts in individual names is high, and in the case of “Refusal to provide true beneficiary explanations and materials,” the vast majority of transfers were from individual accounts.

○ Philippines

The main reasons for the notification of STRs, in order of frequency, are: “Large amount of remittances from a country lacking economic rationality,” “Overseas remittance with false information provided” and “Refusal to provide true beneficiary explanations and materials.” In addition, for “Refusal to provide true beneficiary explanations and materials,” all transfers were made from accounts in individual names.

(B) Reasons for Submitting STRs

Suspicious indicators in cross-border transactions included cases where the purpose of the remittance or the source of funds could not be reasonably explained, where repeated remittances were made to countries or regions unrelated to the stated business activities, and where transactions appeared to route funds through high-risk or third countries. These patterns suggest the possibility that the transactions were intended to transfer criminal proceeds abroad or to obscure the origin and flow of funds.

In terms of reasons for submitting STRs regarding cross-border transactions, the following reports focused on transactions with countries/regions where appropriate measures are not being taken, cross-border transactions funded by large amounts of cash, and transactions suspected of having false information regarding the purpose or source of funds:

- Regarding the remittance of export proceeds from a foreign country to a corporate account, submitted documents, such as a copy of the export permit, shows that the transit point and export destination are countries/regions with a high ML/TF risk.
- When depositing cash, the depositor presents only a Declaration of Carrying of Means of Payment as documentation to clarify the source of the funds.
- Regarding an application for foreign remittance for the purpose of paying patent fees, the head office of the remittance destination is located in a country/region where foreign exchange transactions are restricted.
- Regarding the large amount of remittance to a foreign country, the rationality of the transaction cannot be confirmed, as the source of funds is cash deposits and the details of the remittance purpose are unclear, namely, “aid funds”.
- Regarding large amount of remittances from foreign countries, although the purpose of receipt is declared to be personal funds transfer, the purpose of remittance in the wire is for market research expenses, which shows a discrepancy.
- In the case of multiple large remittances to an account in the name of a legal person whose actual business situation is unknown, the purpose of the remittance was declared to be software fees, but there is no evidence that this is rational given the industry of the transferring legal person, source of funds, and past transaction history, and there is also the possibility of intentionally splitting the transactions, making these transactions unnatural.

(ii) Measures to Mitigate Risks

(A) Statutory measures

○ Act on Prevention of Transfer of Criminal Proceeds

  - Stipulates that specified business operators must verify the purpose of a transaction when conducting a specific transaction[*1].
  - Stipulates that financial institutions that conduct exchange transactions have certain obligations, such as: when establishing correspondent banking relationships with a foreign-exchange transaction operator, they must confirm that such operator has an appropriate internal control system; when making a request to a respondent institution regarding a foreign-exchange transaction involving a cross-border remittance, they must provide information regarding the customer (remittance requester) and the other party of the payment to the institution; and, they must preserve customer identification matters provided by a foreign-exchange transaction operator whose country has similar legislation.

---

*1 Specific transactions as defined in Article 4, Paragraph (1) of the Act on Prevention of Transfer of Criminal Proceeds.

○ FEFTA and Customs Act

- To mitigate the risk related to cash couriers, the FEFTA requires those who export or import cash, the means of payment such as checks, or securities exceeding the equivalent of 1 million yen (100,000 yen in a case bound for North Korea), or over 1 kg of precious metals*[1] to file a notification to the Minister of Finance in writing. The Customs Act also requires that export or import declarations of goods mentioned above to the Director-General of Customs must be made in writing.

(B) Measures by competent authorities

○ Financial Services Agency

- In the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism," the Financial Services Agency disclosed to the public the "required actions" to be taken at the time of execution of correspondent contracts, and the Supervision Guidelines for deposit-taking institution specified the points to consider when supervising the execution of correspondent contracts.
- The Agency has been strengthening its supervisory initiatives with a focus on remittance transactions such as cross-border remittances. Activities include conducting a survey of deposit-taking institutions and funds transfer service providers on remittance transactions.

○ Ministry of Finance

- Specified the details of inspection related to the development of systems necessary to promote the compliance with the FEFTA in the Guidelines for Foreign Exchange Service Providers on Compliance with the Foreign Exchange Act and Its Regulations.
- At customs, the authority conducted lectures and distributed leaflets to the Japanese Bankers Association and others, alerting them to exercise caution and adopt a careful approach when there are requests for large cash deposits or remittances that rely solely on the Declaration of Carrying of Monetary Instruments, etc. as supporting documentation.

(C) Measures by business operators

Examples of specified business operators' measures to mitigate the risk are as follows:

- Conducting interviews and inquiries into the business activities of corporate clients initiating foreign exchange transactions, including visiting the corporate entity and regularly verifying commercial flows and the contents of financial statements after the commencement of transactions.
- Declining transactions involving substantial cash importation or actual cash transactions, such as those involving cash deposits at ATMs, when the rationality of cash transactions is absent.
- For foreign exchanges, verifying not only the purpose of the transfer but also the recipient's use of the funds, and if any discrepancies are found, refusing the transaction or submitting STRs.
- To strengthen verification at the time of transaction for overseas remittance to areas close to countries and regions for which countermeasures were requested from member countries in the FATF statement.
- For corporations providing services that enable foreign remittances via online banking, reviewing their organizational framework annually to determine whether the service can continue to be offered.

---

*[1] bullion made of gold with a gold content of 90% or more by total weight.

(iv) Assessment of Risks

In cross-border transactions, it tends to be more difficult to grasp and trace the flow of transferred funds compared to domestic transactions because of the structural factors, such as the difference in legal systems and transaction systems between countries/regions, and the fact that domestic monitoring and supervision do not extend to other countries.

In fact, there are some cases confirmed that ML has been conducted through cross-border transactions. Considering these situations, it is assessed that cash transactions are a type of transaction carrying a high risk of being misused for ML/TF, and therefore are of high risk

Looking at recent trends in organized crime in Japan, there are confirmed cases where the criminal proceeds obtained by Anonymous and fluid criminal groups and Crime groups of foreigners in Japan were transferred back to foreign countries, demonstrating the risk of illicit fund transfers through cross-border transactions.

Furthermore, considering the situations that increase the risk of ML/TF as indicated in the Interpretive Notes to the FATF Recommendations, as well as examples of actual cases, it is recognized that the following types of transactions among cross-border transactions present higher risk of being misused for ML/TF and are of high risk:

- Transactions related to countries and regions where proper AML/CFT measures are not implemented.
- Cross-border remittances originated from large amounts of cash (or large cash withdrawals immediately after receipt).
- Transactions in which it is suspected that the customer is providing false information about the purpose or source of funds for a cross-border remittance.

[Topic] Analysis of Trade-Based Money Laundering (TBML)

Concealing the fact that funds are criminal proceeds and transferring value through trade transactions is referred to as "Trade-Based Money Laundering" (TBML). Specifically, methods include falsifying export or import declaration details, such as the price, quantity, or description of goods, in trade transactions to make criminal proceeds appear legitimate and transferring them through trade. As a recent trend in Japan, it has also become common to convert proceeds from online and telephone fraud into goods, export those goods, and then recover the sales proceeds locally. Examples of such goods include generally high-value used cars, used pianos, precious metals, cosmetics, and trading cards, as well as in-demand and easily resold Japanese-made clothing and sanitary goods.

An example involving used cars is shown in Table 61.

The funds transferred by victims of online and telephone fraud are routed through multiple bank accounts controlled by the suspects before being deposited, as payment for used cars, into the accounts of business operators engaged in the sale and export of used cars (hereinafter referred to as "used car dealers").

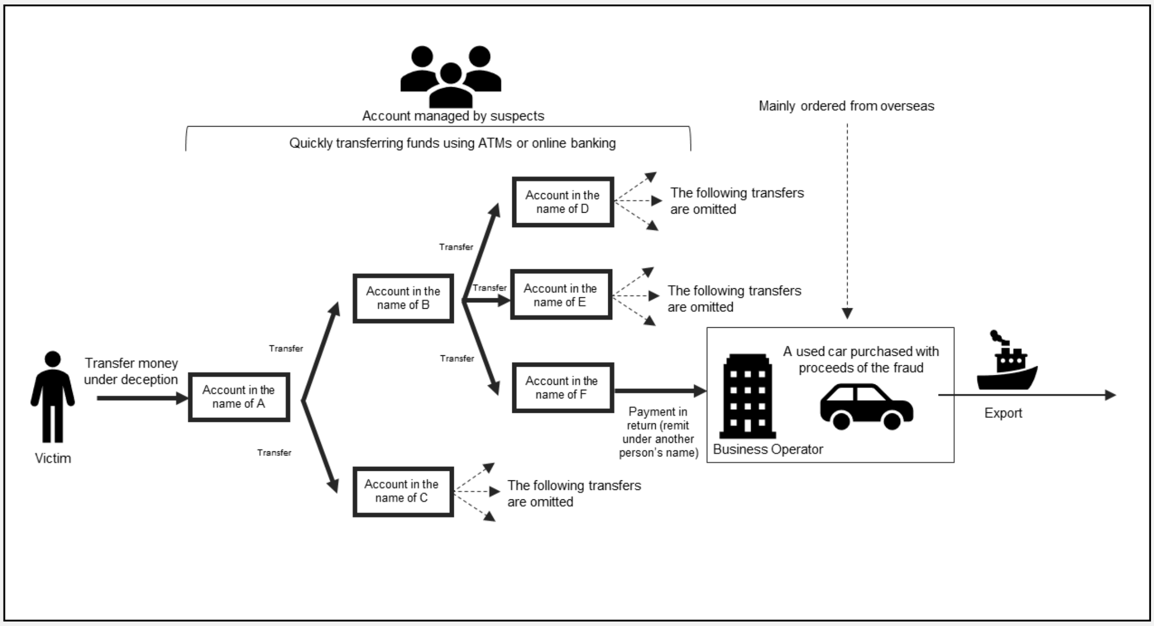
An analysis of the flow of funds revealed several characteristics.

First, large amounts of funds are transferred to used car dealers within a short period of time after passing through multiple bank accounts. In one case, approximately 30 minutes elapsed between the victim's payment of funds in online and telephone fraud scheme and the deposit into the used car dealer's account, during which the funds passed through three bank accounts.

Second, bank accounts in the names of foreigners are primarily used, with a relatively high proportion involving Vietnamese nationals in particular. There have also been cases where bank accounts belonging to individuals who had already returned to their home countries were used. In addition, when funds are deposited into the used car dealer's account, it is often observed that the account name is altered to another foreign name or to a string of numbers.

In light of the above, where numerous bank accounts in the names of foreigners are systematically managed and used for illicit fund transfers. This suggests that, in addition to further strengthening customer due diligence by financial institutions, more agile cooperation between investigating authorities and financial institutions is required, such as facilitating various inquiries necessary for tracing criminal proceeds.

Table 61: Trade-Based Money Laundering



[Topic] Threats of International Fraud and ML Based in Southeast Asia

The United Nations Office on Drugs and Crime (UNODC), in its report published in April 2025 entitled "Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia," revealed that scam centers based in Southeast Asia function as major money laundering hubs, handling an estimated US$40 billion, under structures combining human trafficking, forced labor, cryptoassets, underground banking, and related mechanisms

The report points out the following:

- In special economic zones in Southeast Asia and elsewhere, large-scale scam groups equipped with cyber capabilities have expanded their influence, replacing previously independent and scattered fraud groups. These scam centers operate under the guise of themselves as industrial parks, casinos, hotels, and similar facilities.
- As governments have heightened their sense of crisis, criminal organizations have expanded their areas of operation into neighboring regions with high vulnerabilities, resulting in hundreds of large-scale fraud cases generating tens of billions of dollars in annual profits. Countries in East and Southeast Asia are estimated to have lost up to US$37 billion to cyber-enabled fraud in 2023, with even greater estimated losses reported globally.
- As the online criminal industry in Southeast Asia continues to expand, dedicated business parks serving as operational bases have been developed. In recent years, law enforcement actions have been taken against major bases in Cambodia, the Philippines, Laos, Myanmar, and Thailand.
- A characteristic of the online criminal industry in Southeast Asia is its mobility. Due to external factors such as law enforcement pressure and conflict, operations and workers relocate within countries or across borders (the report includes locations of scam centers identified or reported in the Mekong region).
- The development of fraud bases extends beyond physical infrastructure, with criminal infrastructure also being established, including online gambling platforms, software services, and encrypted, Telegram-based platforms.
- In particular, Huione Guarantee, recently renamed Haowang and originating from Cambodia, has emerged as one of the world's largest illegal online marketplaces in terms of user numbers and transaction volume, serving as a key infrastructure facilitating cyber fraud in Southeast Asia. Cryptoasset wallets used by this platform and its vendors have received at least US$24 billion over the past four years, with an additional US$6 billion flowing primarily through Telegram bots associated with illegal online gambling, potentially being misused for ML[*1].
- Japan has been significantly affected by the expansion of cyber-related fraud and the online gambling industry in Southeast Asia, with funds moving illicitly between the two.
- In recent years, law enforcement agencies worldwide have noted the growing cooperation, partnerships, and synergies between Asian ML organizations and criminal groups across the globe, such as South American drug cartels and the mafias in Italy and Ireland. ML methods by Chinese and other Asian criminal networks are diversifying, including mirror trades[*2], international money mules[*3], so-called "motorcade networks"[*4] (organized networks of money mules), casino junkets[*5], and online gambling schemes.

[*1] In March 2024, the National Bank of Cambodia revoked Huione Pay's banking license. In May 2024, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) designated the Huione Group and its affiliated companies as a "Financial institution of primary money laundering concern."

[*2] A practice in which, almost simultaneously, financial instruments are sold in one country or region and the same number of financial instruments are purchased in another country or region, thereby transferring value on the surface without involving a direct movement of funds.

[*3] A person who transfers criminal proceeds on behalf of another person. In many cases, they receive rewards, although they may not be aware that the funds involved are criminal proceeds.

[*4] A network structure considering of multiple money mules who transfer criminal proceeds continuously or in an organized manner. By cooperating with other criminal organizations in the transfer of criminal proceeds, they aim to obstruct investigations.

[*5] An agent who recruits or refers players to a casino.

2. Countries/Regions

By referring to situations that increase the ML/TF risks listed in the Interpretive Notes to the FATF Recommendations (countries identified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems), countries/regions that require attention because they may influence transaction risks were identified. Then, they were analyzed and evaluated from the perspective of factors that increase risks and measures to mitigate risks.

(1) Factors that Increase Risks

The FATF identifies jurisdictions (countries/regions) with strategic AML/CFT deficiencies that have not made sufficient progress in addressing those deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies. It also issues public statements that call on its member countries/regions to take AML/CFT measures in consideration of risks arising from the deficiencies, and strongly urges all countries/regions to do the same. Those countries/regions identified as High-Risk Jurisdictions subject to a Call for Action*[1] have been published as the “blacklist.”

An FATF public statement is adopted at FATF plenary meetings that are held every four months (normally in February, June, and October). Because identified countries/regions may change each time, specified business operators should continue paying attention to the latest statement.

(i) North Korea

Since February 2011, the FATF has continuously called on its members countries/regions to apply countermeasures, and has strongly urged all countries/regions to do the same, to protect the international financial system from the ongoing and substantial ML/TF risks emanating from North Korea.

(ii) Iran

Since February 2009, the FATF continuously called on its members countries/regions to apply countermeasures against Iran, and has strongly urged all countries/regions to do the same. However, in June 2016, the FATF, taking into account the measures taken by Iran, suspended the countermeasures for 12 months. In June 2017, the FATF decided to continue the suspension of countermeasures and monitor the progress of Iran’s actions, and requested all of its members and other countries/regions to conduct enhanced CDD as appropriate in response to the risks from Iran. In addition to the above request, in October 2019 the FATF asked its members, in line with the FATF Recommendation 19, to strengthen their oversight of branches and subsidiaries of financial institutions based in Iran, to require financial institutions to introduce a reporting system or systematic reporting pertaining to transactions involving Iran, and to require financial groups to undertake an enhanced external audit of all branches and subsidiaries located in Iran. From February 2020, the FATF requests all member countries/regions, as well as other countries/regions, to completely terminate the temporary suspension of the countermeasures against Iran and apply countermeasures, in light of Iran’s failure to develop internal collateral laws for executing the United Nations Convention against Transnational Organized Crime as well as international agreements relating to the prevention of the provision of funds for terrorism, in accordance with the FATF standards.

---

*[1] “High-Risk Jurisdictions subject to a Call for Action” refers to countries/regions that have been publicly identified in an FATF statement as having serious strategic deficiencies in their frameworks for combating ML/TF and proliferation financing.

(iii) Myanmar

Since October 2022, the FATF, considering that Myanmar has not made significant progress in addressing serious deficiencies in AML/CFT measures, has called upon member countries/regions to apply enhanced CDD measures commensurate with the risks emanating from Myanmar, and has strongly urged all countries/regions to do the same.

(2) Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds and its Enforcement Order stipulates that Iran and North Korea are jurisdictions deemed to have inadequate AML/CFT systems (hereinafter referred to as "specified jurisdictions") and requires specified business operators to conduct enhanced CDD when conducting a specified transaction with a person who resides or is located in a specified jurisdiction or a transaction that involves the transfer of property to a person who resides or is located in a specified jurisdiction. It also requires the verification of the status of assets and income if the transactions involve the transfer of property of more than 2 million yen, in addition to the verification of identification matters.

Furthermore, transactions with Myanmar fall under the category of "those that are deemed to have high risk of ML/TF according to the level of risks prescribed in the NRA-FUR" under the Ordinance for Enforcement of the Act on the Prevention of Transfer of Criminal Proceeds. Therefore, in accordance with the Ordinance, the specified business operators are required to conduct enhanced CDD by comparing the natures of transactions with those of usual transactions, making inquiry for the customer, etc. or representatives, etc., conducting necessary examination, and obtaining an approval of a senior compliance official, and to determine whether there is any suspicion of ML/TF on the transaction.

Competent authorities notified specified business operators of the FATF statement and tasked them to fully implement the duties of verification at the time of transaction and STR submission, as well as the duties of giving notice related to foreign-exchange transactions under the Act on Prevention of Transfer of Criminal Proceeds.

For specified business operators to establish and develop a system to submit STRs, the Financial Services Agency's Guidelines for Supervision stipulate areas of oversight requiring special attention. These include giving ample consideration to the modes of transactions (for example, payment amount, the number of times) together with cross-checking nationality (for example, jurisdictions identified by the FATF as uncooperative in implementing AML/CFT standards), and other relevant details, in addition to taking into account the content of this NRA-FUR.

(3) Assessment of Risks

As mentioned in the previous section, it is recognized that international transactions present risks of misuse for ML/TF. Based on the FATF public statements, we understand that transactions related to Iran or North Korea is assessed as posing very high risks.

In addition, we understand that transactions related to Myanmar, which were newly added as High-Risk Jurisdictions subject to a Call for Action in the October 2022 FATF public statement, are also assessed as having a high level of risk[*1].

Even so, the FATF published the names of countries/regions that have serious strategic deficiencies related to AML/CFT measures and have developed action plans to deal with them as countries/regions designated as the Jurisdictions under Increased Monitoring for improving the AML/CFT measures. The FATF is calling on those countries/regions to promptly put those plans into action within the proposed periods of time. Therefore, transactions conducted with those countries/regions before the deficiencies pointed out by FATF are resolved are recognized to be risky.

[*1] Refer to https://www.mof.go.jp/international_policy/convention/fatf/index.html for more information.

Moreover, even if there are no direct transactions with these high-risk countries/regions, malicious and sophisticatedtactics may be used to ultimately redirect funds through neighboring or other countries/regions Therefore, n light of such risks, it is necessary to appropriately implement measures, including verification at the time of transactions.

[Topic] Changes in Countries/Regions for Which the FATF Requested Its Member countries/regions to Apply Countermeasures in the FATF Statements or Designated as under the FATF's Monitoring Process to Improve AML/CFT Measures

Countries/regions considered as risk-increasing factors change in response to the FATF Statement . Therefore, it is necessary to pay attention to the FATF Statement and the results of the FATF meetings. The following list shows when decisions were made and announced between January 2023 and October 2025 regarding countries/regions for which the FATF requested its members countries/regions to apply countermeasures and other measures in the FATF Statements and those designated under the FATF's monitoring process to improve their AML/CFT measures.

Note that countries/regions publicly disclosed at the time of the October 2025 FATF plenary meeting are listed in Table 62 and those that had been disclosed in the past are listed in Table 63, both in alphabetical order.

Table 62: Countries/Regions for which the FATF called on its members countries/regions to apply countermeasures

Legend: ● indicates that the FATF requested its members countries/regions to apply countermeasures, while ◎ indicates that its members countries/regions have been requested to implement enhanced due diligence commensurate with the risk.

Country/Region/	2023			2024			2025		
Period	February	June	October	February	June	October	February	June	October
Iran	●	●	●	●	●	●	●	●	●
North Korea	●	●	●	●	●	●	●	●	●
Myanmar	◎	◎	◎	◎	◎	◎	◎	◎	◎

Table 63: Countries/Regions designated in the FATF's monitoring process for improved observance of AML/CFT measures

Legend: ○ indicates that the FATF designated it for monitoring to improve observance of AML/CFT measures.

Country/Region/	2023			2024			2025		
Period	February	June	October	February	June	October	February	June	October
Algeria						○	○	○	○
Angola						○	○	○	○
Bolivia								○	○
Bulgaria			○	○	○	○	○	○	○
Cameroon		○	○	○	○	○	○	○	○
Cote d'Ivoire						○	○	○	○
DR Congo	○	○	○	○	○	○	○	○	○
Haiti	○	○	○	○	○	○	○	○	○
Kenya				○	○	○	○	○	○
Laos							○	○	○
Lebanese Republic						○	○	○	○
Monaco					○	○	○	○	○
Namibia				○	○	○	○	○	○
Nepal							○	○	○
South Sudan	○	○	○	○	○	○	○	○	○
Syria	○	○	○	○	○	○	○	○	○
Venezuela					○	○	○	○	○
Vietnam		○	○	○	○	○	○	○	○
Virgin Islands								○	○
Yemen	○	○	○	○	○	○	○	○	○
Albania	○	○							
Barbados	○	○	○						
Burkina Faso	○	○	○	○	○	○	○	○	

Croatia		○	○	○	○	○	○		
Cayman Islands	○	○							
Gibraltar	○	○	○						
Jamaica	○	○	○	○					
Jordan	○	○							
Mali	○	○	○	○	○	○	○		
Mozambique	○	○	○	○	○	○	○	○	
Nigeria	○	○	○	○	○	○	○	○	
Panama	○	○							
Philippines	○	○	○	○	○	○			
Senegal	○	○	○	○	○				
South Africa	○	○	○	○	○	○	○	○	
Tanzania	○	○	○	○	○	○	○		
Turkey	○	○	○	○					
Uganda	○	○	○						
United Arab	○	○	○						

* For the situation in each country, refer to the original text of the statement, "Jurisdictions under Increased Monitoring-24 October 2025" (https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-october-2025.html)

[Countries and Regions with Suspended FATF Membership]

The FATF strongly condemned the Russian Federation's aggression against Ukraine. During the FATF plenary meeting in February 2023, it was decided to suspend Russia's membership[*1] in the FATF on the groundthat the Russian Federation's actions unacceptably run counter to the core principles of the FATF, which aim to promote security, safety, and the integrity of the global financial system and represented a gross violation of the commitment to international cooperation and mutual respect. On the other hand, the Russian Federation is still obligated to fulfill the FATF standards and continues to participate as a member of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), maintaining its rights as a member of EAG.

In view of the current international situation over Ukraine, and for the purpose of maintaining international peace and security and contributing to the international efforts for achieving international peace aimed at a solution of the issue, in line with the measures taken by other major countries, Japan has introduced asset freeze measures among other measures under the FEFTA on February 26, 2022, based on the Cabinet Understanding "Asset freeze measures against entities of the self-proclaimed "Donetsk People the 's Republic", self-proclaimed "Luhansk People's Republic," and certain banks in the Russian Federation, prohibitions on imports and exports between Japan and those self-proclaimed entities, prohibition on transactions involving the issuance and circulation of new securities by the Russian Federation government and other governmental agencies, prohibition on the issuance of securities among other measures,by certain banks in Japan, prohibition on the export of items subject to multilateral export control regime to Russian Federation.". .And after that, Japan has continued to work closely with the international community, including the G7, to implement additional financial and trade measures.

[*1] As of June 2025, the FATF comprises 38 member countries/regions, including Japan, as well as two regional organizations (including Russia). Russia has lost the opportunity to participate in discussions and decision-making at FATF meetings due to the suspension of its membership.

3. Customer Attributes

Regarding the customer attributes that affect transaction risks, the following were considered:

- The existence of cleared cases where Boryokudan gangsters or similar actors were arrested for ML offences
- The examples of situations that increase the ML/TF risks listed in the Interpretive Notes to the FATF Recommendations ("non-resident customers" and "ownership structures of companies that appear unusual or excessively complex")
- The matters pointed out in the Third Round of Mutual Evaluation of Japan by the FATF ("a certain measures should be taken in addition to the regular CDD measures if a customer is a foreign PEP" and "secondary supplemental measures should be taken if a document without photo is used for identity verification at the time of transaction," etc. [*1])

Based on these considerations, customer attributes were identified as follows. Then, the above attributes were analyzed and evaluated from the perspective of factors that increase risks and measures to mitigate risks.

Customer Attributes	
An individual attempting to engage in ML	Boryokudan[*2]
An individual whose customer due diligence is difficult to perform	Non-resident customers
	Foreign Politically Exposed Persons (Foreign PEPs)
	Legal persons (legal persons without transparency of beneficial owners)

(1) Boryokudan

Boryokudan is a representative form of organized crime in Japan that commit crime to gain profit in organized and habitual manners.

Boryokudan exist throughout Japan and their size and types of activities are diverse As of June 1, 2025, 25 groups are listed as designated Boryokudan under the Anti-Boryokudan Act.

At the end of 2024, the total number of Boryokudan gangsters was 18,800[*3] including 9,900 Boryokudan members and 8,900 associates[*4]. The grand total of these numbers started to decline in 2005, The figure was the lowest since the Anti-Boryokudan Act became effective in 1992. This is thought to be that withdrawal of members from Boryokudan was encouraged by the intensive law enforcement of the police all over Japan and the progress of

---

[*1] As a result of the amendment to the Act on Prevention of Transfer of Criminal Proceeds in 2014 as well as the amendment to its Enforcement Order and Ordinance associated therewith (enacted in October 2016), it is recognized that the risk that may occur when identification documents without photo are used for identity verification has lowered, however, considering that the identification documents without photo are less credible sources of identity than identification documents with photo, specified business operators need to observe the method of identity verification at the time of transaction under the Act on Prevention of Transfer of Criminal Proceeds and continue to pay attention to the risk of misuse for ML/TF when a customer intentionally refuses to present an identification document with photo.

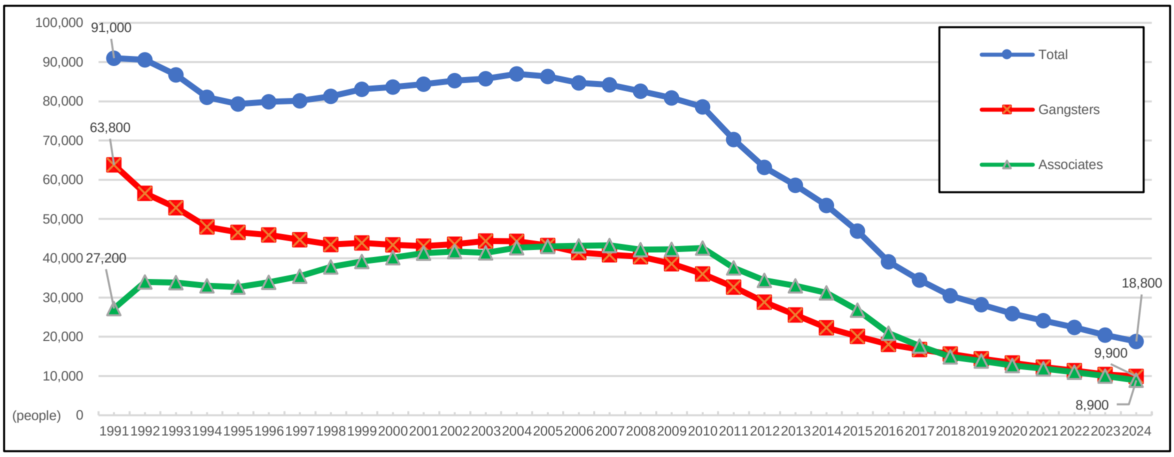
[*2] The major offenders engaged in ML in Japan are analyzed in Chapter 3, where "Anonymous and fluid criminal groups," "Boryokudan," and "crime groups of foreigners in Japan" are identified. In this chapter, the focus is on Boryokudan, for which countermeasures based on customer attributes are primarily relevant to specified business operators. For "Anonymous and fluid criminal groups" and "crime groups of foreigners in Japan," which are not discussed in this chapter, it is also important to implement risk mitigation measures by focusing on their revenue-generating activities and instances of misuse of products and services offered by specified business operators

[*3] The number of Boryokudan gangsters in this section is an approximate figure

[*4] Persons affiliated with Boryokudan other than Boryokudan members, who are likely to commit violent wrongful acts by utilizing the power of Boryokudan, or cooperate or are involved in the maintenance or operation of Boryokudan by offering funds or weapons to Boryokudan or Boryokudan members.

measures to exclude Boryokudan from society.

Table 64: Trends in Boryokudan Gangsters



On the contrary, the number of those who have strong connection with Boryokudan yet do not formally belong to organizations appears to be increasing and there is variation in the activities of those Boryokudan related parties and how they are involved with Boryokudan.

In addition, the groups consist of people who are habitually involved in violent and illegal activities, whereas they do not have firm organizational structure as Boryokudan do, are defined as "quasi-Boryokudan" and criminal groups with features not existing before emerged in recent years, which poses a threat to public safety. The police categorize these groups, including quasi-Boryokudan, as "Anonymous and fluid criminal groups*[1]" and are promoting. It is confirmed that part of the money belonging to some Anonymous and fluid criminal group flows into the Boryokudan; some Boryokudan gangsters are accepted as the leaders or members by Anonymous and fluid criminal group; and Anonymous and fluid criminal group and Boryokudan committed a crime on a conspiracy.

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Boryokudan have been committing various fund acquisition offences according to the changing times, such as the trafficking of stimulants, gambling, collection of protection money from restaurants downtown, intimidation and extortion against companies and administrative agencies, robbery, theft, online and telephone fraud, fraud misusing public benefit programs, and gold smuggling. Moreover, Boryokudan commit crimes to obtain funds, disguising their activities as ordinary economic transactions by using Boryokudan-affiliated companies that Boryokudan substantially control the management or by conspiring with persons who cooperate with or assist in money-making activities *[2] of Boryokudan to conceal their actual state, and their funding activities have become more sophisticated. It is increasingly difficult to define them. Boryokudan groups often conduct ML to avoid tracing of funds, taxation, and confiscation or to avoid being arrested for acquired funds, which blurs the relationship between individual fund-raising activities and funds acquired from such activities.

*[1] The actual situation of Anonymous and fluid criminal groups is described in "1. Offenders, (1) Anonymous and fluid criminal groups in Section 3. Analysis of Money Laundering Cases" in this NRA-FUR.

*[2] Persons who take advantage of the physical power, information power, financial power of Boryokudan to increase their own profits by providing benefits to Boryokudan.

Criminal proceeds are used not only as operational funds to maintain and strengthen the organization or to obtain weapons, but also to interfere with legal businesses, posing a significant threat to the soundness of society and the economy.

As of the end of 2024, the number of cleared cases of ML involving Boryokudan gangsters increased in 2024 compared with the previous year while the total number of Boryokudan gangsters is decreasing. It has also been confirmed that Boryokudan and Anonymous and fluid criminal groups collude with each other to obtain funds while evading restrictions under the Anti-Boryokudan Act and the Organized Crime Exclusion Ordinances. This suggests that ML continues to be an indispensable means for Boryokudan gangsters and similar actors to hinder investigating authorities from tracing their funds.

(B) Typologies

The main cases of ML involving Boryokudan gangsters and similar actors are described in this report under "Chapter 3: Analysis of Money Laundering Cases," Section 1 "Offenders," (2) "Boryokudan."

(ii) Trends of STRs

The number of STRs submitted from 2022 to 2024 was 2,141,107, including 164,086 STRs submitted for reasons related to Boryokudan, accounting for 7.7% of the total number of STRs.

(iii) Measures to Mitigate Risks

Guidelines for How Companies Prevent Damage from Anti-Social Forces (agreed on June 19, 2007 at a working group of the Ministerial Meeting Concerning Measures Against Crime) was formulated to help companies to cut any relationships with Boryokudan[*1].

The Financial Services Agency has formulated the Supervisory Guidelines and related measures for deposit-taking institutions based on the principles outlined above. These guidelines require such institutions to 1) develop a system to take measures as an organization, 2) establish a centralized management system with a department in charge of handling anti-social forces, 3) conduct appropriate preliminary examinations, 4) conduct appropriate subsequent examinations, 5) cut off any relationship with anti-social forces, 6) prevent unreasonable demands made by anti-social forces, and 7) manage shareholder information effectively.

Also, deposit-taking institutions are introducing clauses to exclude Boryokudan into their transaction terms and conditions. This is part of the effort to dissolve business relationships in case a customer has turned out to be Boryokudan. Furthermore, if a customer turns out to be a member of Boryokudan, financial institutions shall consider preparing STRs under the Act on Prevention of Transfer of Criminal Proceeds as a general business practice.

Some specified business operators regularly screen their customers using domestic and foreign databases at the start of transactions and even after the start of transactions. If a customer turns out to be a member of Boryokudan, STRs are submitted.

To thoroughly eliminate Boryokudan from bank loan transactions, in January 2018, the National Police Agency started the operation of a system to respond to inquiries from the banks through Deposit Insurance Corporation of Japan about the correspondence between applicants of new personal loan transactions and Boryokudan information.

(iv) Assessment of Risks

In Japan, Boryokudan engage in various crimes to gain profit, as well as fund-raising activities in disguise of

---

[*1] These include Boryokudan, Boryokudan-affiliated companies, sokaiya (corporate racketeers), person(s) engaging in criminal activities under the pretext of social campaigns or political activities, and violent groups/individuals specializing in intellectual crimes.

legitimate business operations, or misusing business activities. As ML makes the source of proceeds obtained from criminal activities or fund-raising activities unclear, ML is indispensable to Boryokudan and has been confirmed to actually be conducted. Since Boryokudan engage in ML, transactions with Boryokudan are considered to present high risk.

In recent years, Boryokudan are actively engaging in activities to obtain funds in society while concealing the state of their organizations. It has also been confirmed that Anonymous and fluid criminal groups carry out their illegal revenue-generating activities, such as online and telephone fraud, while coexisting and prospering with Boryokudan. In light of these situation, it is necessary to thoroughly examine CDD not only the apparent transaction counterparties, but also to any substantive counterparties.

(2) Non-resident Customers

(i) Factors that Increase Risks

In the Interpretive Notes to the FATF Recommendations, the FATF states that non-resident customers potentially present a high risk of ML/TF.

Specified business operators may conduct transactions with non-residents, including foreigners who do not have addresses in Japan. Generally, the CDD measures, including identification matters and verification of assets and income, for non-residents tend to be limited compared to those for residents. In particular, if specified business operators conduct transactions without meeting the customers, they cannot verify the identification documents of customers directly. In addition, specified business operators may not have the knowledge needed to appropriately determine whether or not identification documents or supplementary documents are authentic if such documents are issued by foreign governments. Therefore, there is a higher risk of specified business operators conducting transactions with customers who are lying about their identification matters when dealing with non-residents compared to residents.

(ii) Measures to Mitigate Risks

The Financial Services Agency's Guidelines for Supervision requires specified business operators to develop internal control systems for suitable examination and judgment in order to submit STRs. Such controls include detailed consideration of customer attributes and the circumstances behind transactions.

In addition, specified business operators implement certain risk mitigation measures for non-resident accounts and transactions, such as setting stricter conditions compared with resident customers, from the perspectives of verification at the time of transaction and transaction monitoring.

(iii) Assessment of Risks

In the case of transactions with non-resident customers, specified business operators tend to have limited measures to conduct ongoing CDD compared with customers residing in Japan. Furthermore, when non-face-to-face transactions are conducted or when identification documents issued by foreign governments are used, anonymity will increase, and it is more difficult to track funds if ML/TF or the like is performed. Therefore, it is recognized that transactions with non-resident customers present a high risk in terms of ML/TF.

On the other hand, in Japan, non-resident account openings and transactions are required to be handled with greater caution compared with those of residents, in accordance with the associated risks. This aspect contributes to a certain extent to the mitigation of risk.

Taking these into account, while the risk in transactions with non-residents may vary depending on the conditions, such transactions are generally assessed as high risk.

(3) Foreign Politically Exposed Persons

(i) Factors that Increase Risks

Foreign politically exposed persons (foreign PEPs: heads of state, senior politicians, senior government, judicial or military officials) have positions and influence that can be misused for ML/TF. When conducting transactions with foreign PEPs, specified business operators' CDD, including verifying customer identification matters and ascertaining the nature/transfer of their assets, is limited because they are sometimes non-resident customers, or even if they are residents, their main assets or income sources exist abroad. On top of that, the strictness of laws against corruption varies from jurisdiction to jurisdiction.

The FATF requires specified business operators to determine whether customers are foreign PEPs and, if they are, to conduct enhanced CDD, including verification of assets and income. In January 2013, the FATF established guidelines on PEPs and expressed its opinion that PEPs present potential risks of committing ML/TF or predicate offences, including embezzlement of public funds and bribery, because of their position. Business operators should, therefore, always treat transactions with PEPs as high-risk ones, regardless of each person's situation.

Bribery, embezzlement of property, and other corruption related to public officials affect the entire society and economy. The international community recognizes that a comprehensive and extensive approach, including international cooperation, is necessary to promote efficient measures to prevent corruption and is calling for measures to prevent the transfer of proceeds derived from corruption by foreign public officials. The Convention on Combating Bribery of Foreign Public Officials in International Business Transactions was adopted by the Organization for Economic Cooperation and Development (OECD) in 1997 with the recognition that unfair competition caused by bribery of foreign public officials should be prevented. In Japan, the amended Unfair Competition Prevention Act (Act No. 47 of 1993) was promulgated in 1998 and prohibitions on providing illicit profits to foreign public officials were introduced, which came into effect in February 1999.

As of now (October 2025), no specific cases of ML/TF related to foreign PEPs have been reported in Japan. However, in recent years, there have been cases of illegal provision of benefits for foreign public servants in violation of the Unfair Competition Prevention Act, as described below:

- A worker at an overseas subsidiary of a Japanese company gave a set of golf clubs to a foreign government official as bribery.
- A worker at a Japanese company abroad provided cash to a foreign public official as a reward for awarding a road construction work tender in an Official Development Assistance (ODA) project.
- A worker at an overseas subsidiary of a Japanese company handed cash, etc., to a local customs official in reward for ignoring illegal operations by the company.
- An employee of a Japanese company handed cash to a foreign public official in reward for concluding an advantageous contract regarding consultation services for railroad construction in an ODA project.
- A former director of a Japanese company provided cash to a foreign public official as a reward for ignoring the company's breach of conditions in connection with the construction business of a thermal power plant.
- A former president of a Japanese company provided cash as a bribe to a local foreign customs official as a reward for reducing the additional taxation and fines for customs clearance.
- Foreigners residing in Japan provided cash to consuls of their consulate in Japan in exchange for issuing the documents needed to apply for statuses of residence and to submit notifications of marriage.
- An executive of a Japanese company provided cash to a foreign public servants in return for reductions or exemptions of fines and additional taxation.

(ii) Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds, as well as its Enforcement Order and Ordinance require specified business operators to conduct enhanced CDD, including verifying customer identification matters, when conducting specified transactions with the following people:

(1) The head of another country or a person who holds or used to hold an important position in a foreign government;

(2) Any family member of (1); or

(3) A legal person whose beneficial owner is either (1) or (2).

Furthermore, these regulations also require specified business operators to verify the status of assets and income if the transactions involve the transfer of property of more than 2 million yen.

In addition, the Financial Services Agency’s Guidelines for Supervision stipulate that one of the focal points for oversight is whether business operators have developed internal control systems to conduct CDD, including verification at the time of transactions appropriately when performing transactions with the head of a foreign country, etc. set forth in the Enforcement Order and Ordinance of the Act on Prevention of Transfer of Criminal Proceeds.

These measures help ensure that the risks of ML/TF are appropriately managed even in transactions involving Foreign Politically Exposed Persons (Foreign PEPs).

(iii) Assessment of Risks

Foreign PEPs have positions and influence that can be misused for ML/TF. In addition, obtaining accurate information regarding their identification matters, as well as the nature and movement of their assets, tend to be difficult, and there are differences among jurisdictions in their efforts to combat corruption. Depending on the situation, it is recognized that transactions with foreign PEPs present a high risk in terms of ML/TF.

(4) Legal Persons (Legal Persons without Transparency of Beneficial Owner)

In the FATF's report*[1] released in 2018, the FATF pointed out that the recent advancement of globalization in economic and financial services offers criminals opportunities to misuse the structure of a company and business to conceal the flow of proceeds and criminality. For example, they conceal illegal proceeds as trading transactions by companies and misuse a dummy or obscure legal person, the nominee system, business operators who provide services for corporations, and thereby conceal the true purpose of the activities of the criminals and beneficial owners. The FATF Recommendations (e.g., Recommendation 24) also requires each country to:

- Ensure that business operators conduct customer identification at the time of the transaction by tracking each customer to a natural person who is a beneficial owner when the customer is a legal person.
- Have mechanisms where the beneficial owner of legal persons can be identified, as well as ensure that competent authorities can obtain or access information on the beneficial owner of legal persons in a timely manner.
- Consider measures to simplify business operators' access to beneficial owner and control information.
- Assess the risk of legal persons with respect to ML/TF.

(i) Factors that Increase Risks

(A) System in Japan

Legal persons in Japan include stock companies, general partnership companies, limited partnership companies, limited liability companies, etc., and all legal persons engaged in these corporate activities acquire legal personality by registering under the Commercial Registration Act (Act No. 125 of 1963). The procedures for establishing a legal person and the matters to be registered vary depending on the type. (See Tables 65, 66, and 67.)

In Japan, there is no nominee system that allows corporate officers or shareholders to be registered under a third party's name; instead, the registered representatives and officers must be recorded using their real names. As a result, compared with other countries, the concealment of a corporation's ownership structure or officer information is unlikely to occur.

Table 65: Number of Corporations by Major Corporate Type in Japan

Category \ Year	2021	2022	2023
Stock company	2,612,677	2,691,378	2,659,393
General partnership companies	3,325	3,068	3,039
Limited partnership companies	12,482	12,290	11,741
Limited liability companies	160,132	184,719	202,723
Others	75,770	22,798	79,821
Total	2,864,386	2,914,253	2,956,717

Note 1: The company sample survey of the National Tax Agency.
2: The number of corporations is the total number of non-consolidated corporations, consolidated corporations, and aggregated corporations.
3: Corporations that are closed or liquidated or general incorporated associations and foundations are excluded.
4: Others refer to cooperative partnerships, special-purpose entities, syndicates, mutual companies, and medical corporations.

*[1] Concealment of Beneficial Ownership (July 2018)

Table 66: Number of Registered Establishments by Each Major Corporate Type

Category \ Year	2022	2023	2024
Stock company	92,371	100,669	98,671
General partnership companies	20	15	11
Limited partnership companies	30	17	19
Limited liability companies	37,127	40,751	41,774
Total	129,548	141,452	140,475

Note: The statistics of the Ministry of Justice.

Table 67: Establishment Procedures and Requirements for Each Major Form of Legal Person

	Stock Companies	Membership Companies		
		General partnership companies	Limited partnership companies	Limited liability companies
Investors	Shareholders	Employees		
Number of investors needed	One or more	One or more (partner with unlimited liability)	One or more of each (partner with unlimited liability and partner with limited liability)	One or more (partner with limited liability)
Scope of liability of investors	Limited liability	Unlimited liability	Unlimited liability/limited liability	Limited liability
Persons responsible for management	Directors	Executive members		
Representative of company	Representative director	Representative member		
Ownership and management	Ownership and management are separated	Ownership and management are the same		
Certification of articles of incorporation	Necessary	Not necessary		
Costs for certification of articles of incorporation	50,000 yen or less	Not necessary		
Registration and license tax	Amount equal to 7/1,000 of initial capital. If the amount is less than 150,000 yen, 150,000 yen.	60,000 yen		Amount equal to 7/1,000 of initial capital. If the amount is less than 60,000 yen, 60,000 yen.
Cost of revenue stamp for articles of incorporation (hard copy)	40,000 yen			
Amount of investment and initial capital	Needs to include initial capital, amount not exceeding 1/2 of which can be recorded as capital reserves.	The entire amount can be recorded as the capital surplus.		

Examination of contribution in kind by company auditor	As a rule, necessary.	Not necessary
Public notice of account closing	Necessary	Not necessary
Profit and loss distribution	As a rule, distributed based on investment ratio.	Unless otherwise set forth in articles of incorporation, distributed based on the value of each member's contribution.
Highest decision-making body	General shareholders meeting	Agreement of all members
Amendment of articles of incorporation	Special resolution at general shareholders meeting	Agreement of all members
Term of office of officers	As a rule, 2 years. 10 years maximum for privately held companies.	None
Transfer of shares (equity)	As a rule, no restriction. Certain transfer restrictions are allowed.	Agreement of all other members

(B) Inherent Risks of Being Misused for ML/TF

Legal persons are entities to which property rights belong independently of natural persons, and are considered to have characteristics unique to legal persons that are different from natural persons, as well as vulnerabilities regarding measures against ML/TF that arise from these characteristics.

Characteristics unique to legal persons	
Structure	● A natural person can change their ownership of property without the cooperation of another natural person by transferring the ownership to a legal person. ● In general, legal persons have complex rights and controls over their assets. In the case of a company, various people, including shareholders, directors, executive officers, and even creditors, have different rights to company assets in accordance with their respective positions.
Transactions	● Having legal personality can provide credibility in transactions. ● Being able to frequently transfer large amounts of assets. ● The impact of a suspension of transactions is greater than for individuals.
Corporation type	● The articles of incorporation necessary for establishing a stock company must be certified by a notary public; however, such certification is not necessary for a holding company. ● When establishing a stock company, a beneficial owner must be identified, but such identification is not necessary when establishing a holding company. ● The procedures for establishing a stock company are strict, therefore it has high general credibility and shares are easy to transfer. ● The establishment procedures for membership companies are generally simple, and maintenance costs are low.
Other	● There are business operators who provide an address, facilities, and means of communication (rental offices and virtual offices), i.e., so-called address rentals. Some of these service providers offer postal receiving services, telephone receiving services, telephone forwarding services, and other additional services. ● It is said to be easy to develop various investment schemes in countries/regions called offshore financial centers, where financial services are provided to foreign corporations and nonresidents at low tax rates due to lax financial regulation.

	● Some countries/regions have adopted the nominee system, under which legal persons' executives and shareholders can be registered in third-party names for privacy protection.

Vulnerabilities regarding measures against ML/TF
● If a property is transferred to a legal person, it enters the complex rights/control structure of a legal person, making the entity to which it belongs unclear and making it difficult to trace criminal proceeds. ● By mixing criminal proceeds with legitimate business earnings, the source of illegal earnings can be made unclear. ● By using services such as rental offices, it becomes possible to provide others with an address or a telephone number that is not actually used by the legal person as its own and make up fictitious or exaggerated appearances of business trustworthiness, and business scale, by using corporate registration. ● There is a risk that shell companies may be established in countries/regions serving as offshore financial centers and that the shell companies are misused to conceal criminal proceeds.

Those who plan ML/TF may attempt to achieve it by misusing these characteristics of legal persons. For example, they may hide behind the complex rights/control structure of a legal person or may substantially control a legal person and its property while obscuring their involvement with the legal person (e.g., placing a third party, who is under their control, as a director of the legal person).

(C) Typologies

Examples of corporate misuse include cases where a shell company is established to open a corporate bank account and conduct rapid inflows and outflows of funds within a short period of time, as well as cases where dormant companies or corporate bank accounts are purchased and used. Other examples include mixing criminal proceeds with revenues of legitimately operating corporations, or conducting money laundering by providing fund transfer services through payment and collection agencies. Funds circulated through these methods have included criminal proceeds related to online and telephone fraud, investment/romance fraud via social media, and online casino activities. These cases demonstrate that situation in which corporations are established or corporate bank accounts are managed by person other than the nominal representatives, as well as cases where corporate activities or fund flows are unclear, can constitute risk factors for ML.

The main examples in which corporations or similar entities with opaque operations were misused for ML are as follows:

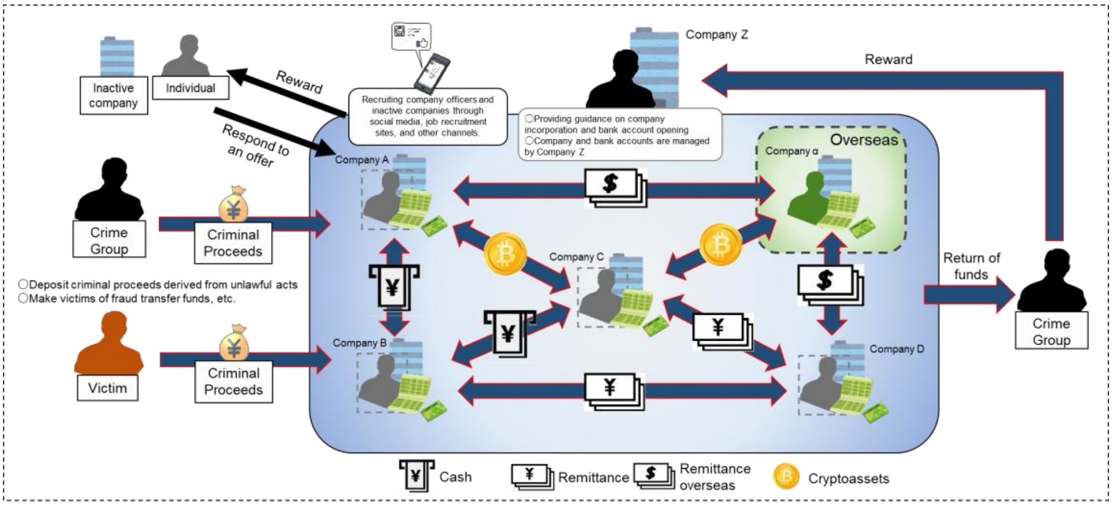
[Case 1]
Using social media and other means, individuals were recruited to act as representatives to establish paper companies, and bank accounts were fraudulently opened in the names of these paper companies. Additionally, under the guise of payment and collection agencies, wagers of online casino were deposited into these accounts, routed through multiple other corporate accounts managed by the criminal group, and ultimately transferred abroad. The accounts managed by the criminal group also received other criminal proceeds, which were moved through foreign remittances, ATM cash withdrawals, and the purchase of cryptoassets.

Furthermore, domestic cleared cases of ML offences involving the misuse of corporations revealed the following realities:

Type of Misused Corporations
● Establish a shell company and use it to receive and transfer funds within a short period of time. ● Acquire an existing corporation owned by a third party and change only the registered representative before using it ● The registered representative differs from the actual controller, effectively "lending" the corporate name ● A legitimately operating corporation cooperates in sending or receiving criminal proceeds at the

request of a third party
Characteristics of Corporate Registration
● Many corporations were found to have relatively small registered capital amounts, ranging from tens of thousands to hundreds of thousands of yen; however, in recent years, corporations with comparatively large amounts of capital have also been used. ● Changes to the registered address or officers occur frequently. ● The registered business purposes are numerous and show little relation to one another. ● The stated business purposes are changed to activities such as service businesses that do not involve physical goods that make it easier to outwardly explain the legitimacy of fund flows.
Trends in Incorporation Methods
● Compared with stock companies, limited liability companies (LLCs) are easier to establish and tend to be misused in a short period. There have been cases where a company was misused within just a few months after its establishment. ● Recently, there have also been numerous cases where established stock companies have had their accounts misused. ● When establishing new companies, there are cases where multiple companies are set up through the same judicial scrivener corporation. ● The establishment of a cooperation itself may be used as a means of transferring criminal proceeds, and corporate accounts may be misused as so-called "tunnel accounts."
Trends in Predicate Offences
● Nearly half of the cases involve fraud. ● In addition, they are frequently used in computer fraud and gambling offense.

Table 68: Illustration of Organized ML Misusing Corporations



The number of cases and the number of corporations in which shell or opaque corporations were misused among ML offences cleared between 2022 and 2024 are shown in Table 69.

Table 69: Number of Cases Where Shell or Opaque Corporations Were Misused/Number of Misused Legal Persons

	2022	2023	2024
Number of cases	6	15	35
Total by type of legal person	11	23	65
Stock companies (including special limited liability company)	9	19	36
Limited liability companies	1	4	29
General partnership companies	0	0	0
Limited partnership companies	0	0	0
Other	1	0	0

(ii) Trends of STRs

Indicators of suspicious transactions related to corporate misuse include the opening of corporate accounts immediately after registration, the concentration of high-value transactions within a short period, transfers or deposits inconsistent with the stated business activities, account operations or withdrawals carried out by persons other than the representative, repeated foreign remittances, and frequent changes to contact information. These signs suggest that the corporation may be misused as a fund collection point or intermediary, in the form of so-called tunnel accounts or payment and collection agency accounts.

The customer attributes, details of business, and forms of transactions related to companies reported as opaque companies or companies with unidentified beneficiaries in STRs are as follows:

- It was discovered that a person holding an account related to an officer or corporation belongs to Boryokudan.
- A representative director of a company, who is a foreigner, is under the status of residence with restrictions on employment.
- There are many unrelated matters to the registered business purpose, and no business activities can be confirmed at the representative's address or the company's location.
- When a transaction was requested, it was discovered that the company representative and address had changed, so submission of documents such as the shareholder register and articles of incorporation was requested, but it was refused, and the beneficial owner is unclear.
- An office or store did not exist at the registered address, or a customer could not be reached at the registered telephone number.
- The same address is used as the registered address of a lot of companies without active business operations, which are suspected to be shell companies.
- A company showing no signs of actual operations had an account in which there were frequent transactions of unclear deposits and withdrawals in cash.
- A bank account in the name of an individual is used for transactions between companies without justifiable reason.
- All of the deposited funds were immediately transferred to another company with the same person as a representative, or an account was suspected to be misused as a dummy account.
- Companies that, shortly after opening an account, frequently change their registered addresses and have frequent changes in their representatives, leading to opacity in identifying the beneficial owners.
- The representative was unable to provide a clear explanation of the business, and a third party was involved in the negotiations, raising doubts about the beneficial owner.
- There was a sudden high-value transaction on the account of the cryptoassets exchange service provider, and there were also signs of multiple terminals being used to share information such as IDs and passwords required for login.

(iii) Measures to Mitigate Risks

To prevent legal persons from being misused for ML/TF, it is important to ensure that the legal persons are transparent and that their funds are traceable by revealing their beneficial owners. It is also important to understand the characteristics unique to legal persons and implement appropriate measures such as verification at the time of transaction.

In light of the FATF Recommendations, as well as the adoption of the G8 Action Plan Principles during the Lough Erne summit in June 2013, Japan has so far established systems to verify the information on beneficial owners of legal persons.

Statutory measures	
Act on Prevention of Transfer of Criminal Proceeds and its Ordinance	● Defines a beneficial owner and requires specified business operators to verify the identification matters of a beneficial owner of a customer which is a legal person. ● Requires specified business operators performing services to provide companies with addresses and facilities for business, means of communication, and addresses for management to verify identity and other information when executing a services agreement, and to prepare and preserve verification records and transaction records.
Ordinance for Enforcement of the Notary Act (Order of the Attorney-General's Office No. 9 of 1949)	● Requires notaries to have clients notify the name of a beneficial owner and whether the beneficial owner is a Boryokudan member international terrorist, or a person involved in weapons of mass destruction-related plans when certifying the articles of incorporation upon establishment of a stock company, general incorporated association, or general incorporated foundation.
Regulation on Storage of Beneficial Ownership Information List in the Commercial Registry Office (Ministry of Justice Public Notice No. 187 of 2021)	● Stipulates a system whereby the commercial registry office shall, upon request from a stock company, retain a document containing information on its beneficial owners of a stock company and issue its copy in order to identify the beneficial owner after the corporation's establishment.
Companies Act	● It stipulates the dissolution of companies deemed to be inactive*[1], a system intended to mitigate the risk of inactive companies that have been resold or whose registration has been illegally changed from being misused for crimes. ● Dissolution of inactive companies has been occurring every year since fiscal 2014, with approximately 29,000 cases in fiscal 2022, 28,000 cases in fiscal 2023, and 27,000 cases in fiscal 2024.
Other measures	
● The Financial Services Agency's Guidelines for Supervision stipulate that one of the focal points for oversight is whether an adequate system has been established to conduct verification appropriately at the time of transactions, such as verification of the beneficial owner when conducting transactions with a legal person. ● In "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism," financial institutions are requested to appropriately confirm the identity of the beneficial owner at the time of transaction, not only at the start of transactions but also in ongoing CDD, thus taking measures commensurate with the risk.	

(iv) Assessment of Risks

Due to their unique characteristics, legal persons can easily conceal criminal proceeds, and there is a recognized risk that transactions with legal persons could be misused for ML/TF. In recent years, there have been cases where, even if the ownership structure of a corporation is not complex, its establishment or account management is actually carried out by third parties, or the corporation continues to be used despite its activities and the flow of funds remains unclear.

Looking at the type of corporation, for stock companies, there are cases of misuse of existing corporations due to their high credibility, as well as cases where newly established corporations are misused for ML within a short period. For limited liability companies (LLCs), due to the ease of establishment, misuse tends to occur relatively shortly after incorporation compared to stock companies.

Furthermore, as the FATF points out, for legal persons without transparency of beneficial owners, it is difficult to identify the ownership and flow of funds, making transactions with such corporations particularly risky.

In light of this, when dealing with corporations that combine a lack of substance, unclear management, and opaque fund flows, there is a high likelihood of misuse for ML, and such transactions are assessed to be high risk.

*[1] A stock company for which 12 years have elapsed since the day when activity regarding such stock company was last registered.

[Topic] Analysis of Criminal Groups Engaged in ML Using Corporations

In recent years, it has become evident that there are criminal groups that handle the ML of proceeds from crimes committed by other groups, such as online and telephone fraud, investment/romance fraud via social media, and online casino operations. In 2024, a criminal group was arrested that recruited individuals via social media to act as representatives of shell companies, guided them on the procedures, and had them establish corporations and open corporate accounts, which were then used to launder criminal proceeds. Subsequently, there have also been cases of criminal groups managing multiple corporate accounts and laundering criminal proceeds.

The results of the analysis of the characteristics of the corporations, accounts, and transactions used by these criminal groups are as follows:

1. Analysis Results Concerning Corporations

The analysis results concerning corporations are as follows. It should be noted that the characteristics of misused corporations listed below are based solely on an analysis of certain criminal groups, and the majority of corporations exhibiting these characteristics conduct legitimate business activities. Therefore, it is important to implement measures while keeping in mind that not all corporations with these characteristics should be considered suspicious solely for that reason.

- For corporate type, misuse of stock companies accounted for the majority
- For registered address, many were located in major metropolitan areas. The corporate address appears to be related to attributes such as the residence of the suspect or the corporate representative.
- For type of building for registered address, apartment complexes were the most common, followed by detached houses, while office buildings and rental offices were relatively rare.
- For newly established corporations, the most common capital amount was between 2 million and 3 million yen. The capital often served as a “show money” for incorporation, and withdrawals after establishment were also observed.
- In cases where existing corporations were believed to be misused rather than newly established corporations, the capital amount could reach several tens of millions of yen.
- The majority of corporations listed IT-related activities at the top of their purpose statements, such as internet-based advertising, promotion, content planning, design and development, website production, system development for apps and software, and RPA[*1]. Other purposes included administrative outsourcing such as company or accounting services, those related to intellectual property such as intellectual property ownership, licensing and management, sales and marketing outsourcing or advertising agency services, consulting, construction, cleaning, and various payment and collection agency services.
- As for the number of business purposes, most corporations listed 4 to 6 purposes.
- As for the number of executives, the majority had only one executive, who served as both representative director and director.
- Cases where the same representative was in charge of multiple corporations or multiple corporations were established at the same address were relatively rare.

2. Analysis Results Concerning Accounts

(1) Types of Financial Institutions Misused for ML

Among accounts misused for ML, online-only banks were the most common, followed by city banks and regional banks. In cases where groups instructed a single corporation to open accounts at multiple banks, they tended to prioritize opening accounts with online banks and city banks that are well-known, convenient, and allow newly established corporations to open accounts.

(2) Examples of Reasons for Refusal of Account Opening

The criminal groups analyzed in this analysis opened accounts at multiple banks for a single corporation. However, in

[*1] Abbreviation for Robotic Process Automation. Refers to a technology that automates tasks using software robots.

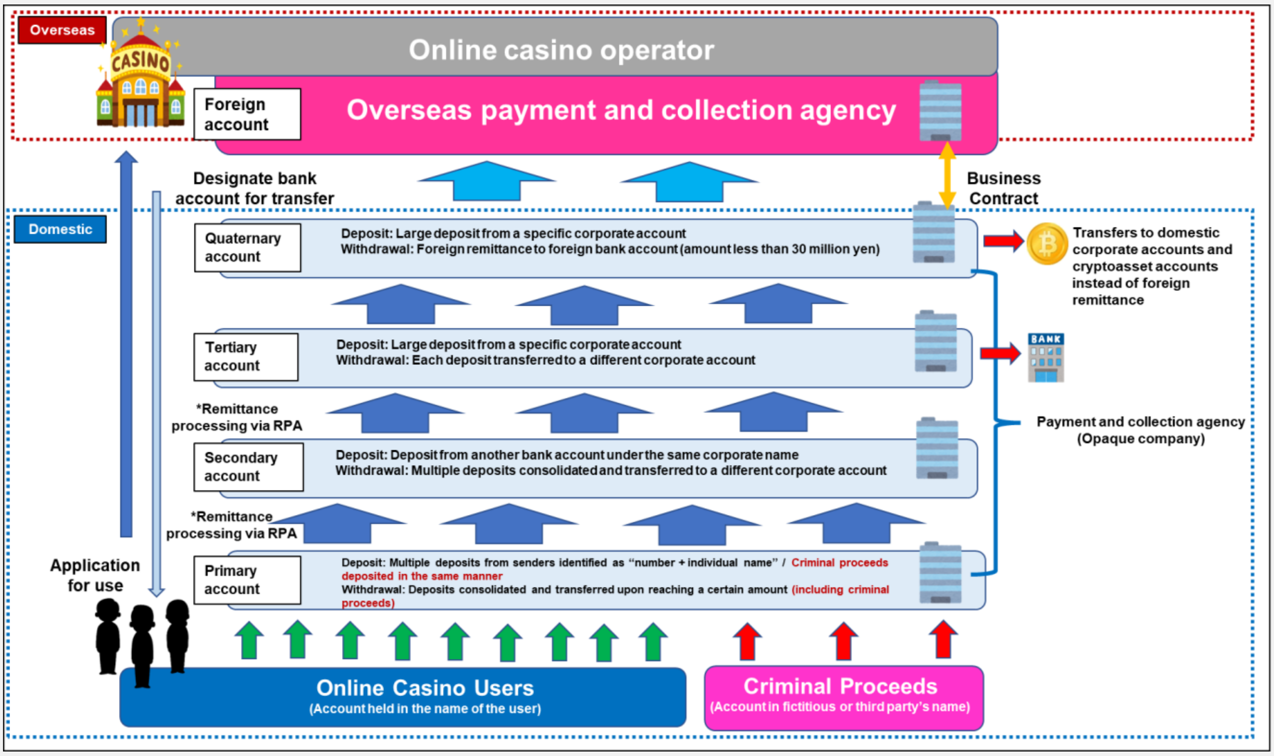
some cases, banks refused to open accounts. Examples of reasons for refusal identified through this analysis are as follows:

- The corporation was recently established, and its business activities are unclear. The corporation already has accounts at other banks, making a new account unnecessary.
- The corporation was recently established, and its registered address corresponds to a virtual office and there are irregularities in its declared business purpose.
- The corporation was recently established, and its website is simplistic, making it difficult to adequately verify the actual business activities.
- The corporation claims to operate event-related businesses, as stated on its website; however, it was recently established and has no clear track record. In addition, the company address and the representative's residence are located in the same office building, raising suspicion.
- The business involves waterproofing work, but the headquarters is located in a single apartment unit, with no apparent storage for construction materials.

3. Analysis Results Concerning Remittance Transactions

Among criminal groups engaged in laundering criminal proceeds, it was observed that funds deposited into an initial account (primary account) were quickly transferred to another account (secondary account), then routed through multiple intermediary accounts (tertiary accounts), and ultimately transferred to an account used for cross-border remittances (quaternary account). Additionally, during this process, some transactions involved transfers to bank accounts of cryptoassets exchange service providers or cash withdrawals via ATMs.

Table 70: Illustration of ML Using Corporate Account (Utilizing the Mechanism of Online Casinos)



(1) Domestic Transactions

a. Main Characteristics Observed in Primary Account Transactions

- Numerous incoming transfers consisting of "numbers only" or "numbers + individual names" (suspected use of online casinos).

- Once the deposited funds reach a certain amount, almost the entire balance is transferred to another account at a different financial institution under the same corporate name.
- Multiple transfers are conducted within a single day.
- In addition to transfers believed to be wagers of online casino, deposits suspected to be criminal proceeds from offences such as fraud are also observed.
- In some cases, RPA is used to automate the transfer process.

b. Main Characteristics Observed in Secondary Account Transactions

- Numerous incoming transfers from other accounts at different financial institutions under the same corporate name.
- The multiple incoming transfers are aggregated and sent to a different account at another financial institution under a different corporate name.
- Most transfer amounts are not round numbers, but include figures down to single-digit units.
- In some cases, RPA is used to automate the transfer process.

c. Main Characteristics Observed in Tertiary Account Transactions

- After receiving transfers of several million yen from a specific corporate account, the same amount is sent on the same day to another account under a different corporate name at a different financial institution.
- After receiving high-value transfers (tens of millions of yen) from a specific corporate account, large sums ranging from tens of millions to hundreds of millions of yen are transferred to another corporate account.
- When transferring to an account for foreign remittances, amounts under 30 million yen are sent via a different corporate account at another financial institution.
- Most transfer amounts are non-round amounts, but include figures down to single-yen digit.

d. Main Characteristics Observed in Cryptoasset Exchange Service Provider Accounts

After receiving transfers ranging from several million to several tens of millions of yen from a specific corporate account, the full amount is transferred each time to a bank account of a cryptoassets exchange service providers.

(2) Foreign Remittances

a. Main Transaction Purpose

Payment for services such as digital content usage fees, website management fees, system service-related costs, advertising and marketing fees, market research expenses, and legal fees.

b. Main Counterparties (Countries/Regions)

Philippines, Singapore, Taiwan, United Kingdom, Germany, and Hong Kong.

c. Main Transaction Characteristics (Amounts and Frequency)

- Repeated transfers of less than 30 million yen.
- The source funds are transfers from specific corporate accounts, and after receipt, the same amount is remitted abroad on the same day or within about three days.
- Frequency is typically once per day, with a maximum of about 10 times per month, and multiple transfers on the same day do not occur.

[Topic] Risk of the Misuse of Legal Arrangements for ML/TF

The FATF, in Recommendation 25, calls on countries to assess the risks of ML/TF associated with legal arrangements and to take appropriate measures. Legal arrangements include, in addition to the trusts handled by trust banks (commercial trusts) discussed in Chapter 5 of this NRA-FUR, civil trusts and foreign trusts. This section analyzes and evaluates the risks of ML/TF associated with civil trusts and foreign trusts[*1]. It should be noted that in some countries and jurisdictions outside Japan, nominee arrangements are legally recognized, and in practice, ML/TF have been conducted by combining nominee arrangements with trust structures. However, there is no nominee system in Japan .

1. Civil Trusts

(1) Characteristics

A civil trust refers to a trust in which the trustee does not act for profit and does not repeatedly or continuously engage in the business of accepting trusts. Civil trusts are generally established through a trust agreement[*2] between family members (relatives), for purposes such as entrusting management and disposition of assets, including money, to a trustee in the event that the settlor's decision-making capacity declines. Additionally, to avoid disputes regarding the validity of the trust agreement, the trust deed is often executed as a notarized document. The trend in the number of notarized documents related to civil trusts from 2018 to 2023 is shown in Table 71.

Table 71: Number of Notarized Documents Related to Civil Trusts[*3]

Year		2018	2019	2020	2021	2022	2023
Civil Trust		2,223	2,974	2,924	3,200	3,960	4,434
Details	Trust Agreement	2,088	2,840	2,768	3,038	3,753	4,179
	Testamentary trust	83	76	65	87	94	150
	Self-settled trust	52	58	91	75	113	105

In civil trusts, cash is the most common type of trust property, followed by real estate (both residential and income-producing properties), with cash included in approximately 90% of trust assets [see Table 72]. While not strictly required under the Trust Act to fulfill the duty of segregation, it is common in civil trusts for the trustee to open a trust account or a dedicated trust account and manage the assets through that account.

Table 72: Types of Trust Assets Included in Civil Trusts[*4]

Type	Percentage
Cash	90%
Residential real estate	43%
Income-producing real estate	48%
Listed shares	2%
Unlisted shares	20%

(2) Measures to Mitigate Risks

Since the trust property in civil trusts is often cash, and trusts that open a trust account at a financial institution are believed to constitute the majority of civil trusts, measures taken by third parties involved in the account opening process, such as notaries, legal professionals involved in drafting the trust agreement, and financial institutions, are considered to contribute to mitigating the ML/TF risks.

2. Foreign Trusts

(1) Characteristics

The Interpretive Note to FATF Recommendation 25 states that countries should assess "foreign legal arrangements that have a sufficient link with their own country." The definition is as follows:

Definition of "Sufficient Link" for "Foreign Trusts" under the Interpretive Note to FATF Recommendation 25 (Legal Arrangements)	
(i)	A trust established under foreign laws where the trustee (or other equivalent person) maintain a significant and on-going business relationship with a financial institution or DNFBPs[*5] in the country."
(ii)	A trust established under foreign laws where the trustee (or other equivalent person) holds significant real estate or other significant investments in the country.
(iii)	A trust established under foreign laws where the trustee (or other equivalent person) is a resident for tax purposes in the country.

In Japan, with respect to foreign trusts defined under items (i) and (ii) above, the survey on the ML/TF risks relating to trusts identified the following circumstances:

(i) According to interviews and other findings from commissioned research, no foreign trust accounts in Japan were identified, and cases where Japanese legal professionals establish foreign trusts are extremely rare.

(ii) When real estate located in Japan is included as trust property, it becomes subject to public registration under laws such as the Real Estate Registration Act (Act No. 123 of 2004), and trust registration is required under the Trust Act. In practice, registering a foreign trust presents many challenges, including the preparation of trust registration documents, translation of trust agreements, and explaining concepts of foreign laws to the Legal Affairs Bureau. Therefore, the survey did not identify specific cases where Japanese professionals established foreign trusts using real estate in Japan as trust property.

Furthermore, regarding foreign trusts defined under item (iii), if the trustee resides in Japan, reporting obligations under income tax and other laws (submission of statutory reports) apply, allowing tax authorities to identify such trusts.

(2) Measures to Mitigate Risks

As noted in (1), due to practical challenges, cases where Japanese legal professionals establish foreign trusts are extremely rare. Even if Japanese real estate is included as trust property in a foreign trust, trust registration ensures a certain level of transparency, which is considered to contribute to mitigating ML/TF risks.

3. Assessment of Risks

Unlike in foreign countries where ML/TF have been carried out through the combination of nominee arrangements and trusts, in Japan, where nominee arrangements do not exist, there have been no detected cases of ML using trusts. Among trusts, the scale of civil trusts is limited compared to "trusts handled by trust banks (commercial trusts)." Regarding foreign trusts, due to practical challenges, cases where Japanese professionals establish foreign trusts are extremely rare, and within the scope of this survey, no foreign trust accounts could be identified.

Therefore, it is assessed that, overall, the risk of civil trusts and foreign trusts being misused for ML/TF in Japan is low.

[*1] In conducting this analysis, reference was made to the results of the Ministry of Finance's commissioned surveys: "Survey on the Money Laundering and Terrorist Financing Risk of Trusts" (March 2025) and "Survey on FATF Recommendation 25 (Legal Arrangements)" (March 2024).

[*2] Article 3 of the Trust Act (Act No. 108 of 2006) stipulates the methods for establishing a trust, including trust agreements, testamentary trusts, and self-settled trusts.

[*3] Quoted from Table 2 of the "Survey on the Money Laundering and Terrorist Financing Risk of Trusts."

[*4] Quoted from Table 3 of the "Survey on the Money Laundering and Terrorist Financing Risk of Trusts." Trust assets may include multiple types of property.

[*5] Abbreviation for Designated Non-Financial Businesses and Professions.

Section 5. Risk of Products and Services

This section assesses the risks of products and services provided by each type of specified business operators. It also analyzes products and services using new technologies that should be monitored closely[*1].

1. Major Products and Services in which Risk is Recognized

When assessing the risk, criminal environment described in "Section 2. Environment Surrounding Japan," major transactions misused for ML and the examples of use of STRs described in "Section 3. Analysis of Money Laundering Cases," and transaction types and risks (non-face-to-face transactions, cash transactions, and cross-border transactions) analyzed in "Section 4. Risk of Transaction Types, Countries/Regions, and Customer Attributes" in this NRA-FUR are considered. The assessment also takes into account the scale of each business type and the vulnerability of each product/service, while analyzing the factors that increase the risks for each product/service provided by specified business operators, details of STRs, and measures to mitigate risks.

The following are the vulnerability factors that present particularly high risks.

Vulnerability factor	Overview
Anonymity	Anonymity of source of funds through cash transactions, anonymity of non-face-to-face transactions in the Internet space, and anonymity through the creation of a fictitious appearance
Transferability	Ease of transferring funds and ease of transferring rights (ownership, beneficiary rights, etc.) to third parties (transfer of rights holders)
Extensiveness	The geographical and attribute extensiveness of the counterparty of the transfer (Cross-border transactions, etc.)
Convertibility	The convertibility of the source of funds, such as the ease of converting cash into other rights or goods, or converting goods with high property value into cash
Complexity	Sophistication and complexity of transaction type that make tracing difficult.

The results of the assessment of risks for each product or service provided by specified business operators are as follows:

Risk level	Products and services
Transactions of relatively higher risk than other business forms	Products/services provided by deposit-taking institutions (excluding those listed in the table below), funds transfer services, electronic payment instruments, and cryptoassets
Transactions considered to be of risk	Insurance, investment, trust, money lending, high-value electronically transferable prepaid payment instruments, foreign currency exchanges, financial leasing, credit cards, real estate, precious metals and stones, postal receiving services, telephone receiving services, telephone forwarding services, and legal/accounting services

[*1] The products and services handled by each specified business operator are described in the NRA-FUR. However, the scope of products and services handled by specified business operators is not uniform. It is necessary for business operators to take the descriptions in the NRA-FUR into consideration according to the products and services they handle.

(1) Products and Services Dealt with by Deposit-taking Institution

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Deposit-taking institutions[*1] such as banks must obtain licenses from the Prime Minister under the Banking Act, etc. As of the end of March 2025, 1,162 institutions have obtained the licenses, etc. They are mainly banks (133 banks, except branches of foreign banks) and cooperative financial institutions (254 Shinkin Banks, 143 Credit Cooperatives, 13 Labour Banks, 578 agricultural cooperatives and fishery cooperatives, and 41 credit federations of agricultural cooperatives and credit federations of fishery cooperatives). Among these institutions, banks held a total deposit balance[*2] of 1,190,122.1 billion yen for a total of 738.10 million accounts as of the end of March 2025.

Acceptance of deposits, loan of funds, discounting of bills, and exchange transactions (domestic and foreign exchange) are inherent business operations*[3] of deposit-taking institutions, which also handle ancillary business such as consultation on asset management, sales of insurance products, credit card services, proposals for business succession, support for overseas expansion, and business matching.

In addition to banking operations mentioned above (including ancillary business), some banks engage in trust business and undertake trust of cash, securities, monetary claims, movables, and real estate as a trust business and also handle business stipulated in the Act on Engagement in Trust Business Activities by Financial Institutions, such as real estate-related business (agency, examinations, etc.), stock-transfer agent business (management of stockholder lists, etc.), and inheritance-related business (execution of wills, disposition of inheritance, etc.).

Deposit-taking institutions in Japan vary in the scale and scope of operation. The Financial Services Agency, which is the competent authority overseeing banks, Shinkin banks, etc., has classified them into major banks (Mega-banks, etc.) and small- and medium-sized or regional financial institutions (regional banks, second-tier regional banks, and cooperative financial institutions) to supervise them. Each of the three Mega-bank groups has branches throughout Japan. They are selected as Global Systemically Important Financial Institutions (G-SIFIs) and are promoting international expansion. Regional banks and second-tier regional banks each have a certain geographic area where they mainly operate, but some regional banks have strategies to expand their business into several regions. Cooperative financial institutions operate in particular districts only.

Deposit-taking institutions have a wide range of customers, from individuals to big companies. They also handle a large number of transactions. As such, it is not easy for deposit-taking institutions to find customers and transactions related to ML/TF and eliminate them.

Furthermore, considering the status and role of Japan as an international financial market, Japan is no exception to the growing threat of ML/TF across the world. As a matter of fact, cases have occurred in which Japan's financial institutions were used as channels for the transfer of funds during the process by which some cross-border crime organizations have laundered proceeds illegally obtained by fraud, etc., in foreign countries.

[*1] Deposit-taking Institutions mean those listed in Article 2, paragraph (2), items (i)-(xvi) and (xxxvii) of the Act on Prevention of Transfer of Criminal Proceeds (banks, Shinkin banks, etc.).

[*2] Based on the Bank of Japan Time-series Data. The Resolution and Collection Corporation and the Japan Post Bank are not included in the Data.

[*3] Business stipulated in the Banking Act, Article 10, paragraph (1), each item.

In light of these characteristics, the Financial Services Agency has assessed that the sector risk of deposit-taking institutions is “High” in its financial sector analysis*[1]. In particular, the Financial Services Agency states that the risk is relatively high for mega-banks that conduct a lot of foreign exchange transactions and correspondent contracts, and Internet-only banks that mainly handle non-face-to-face transactions.

(B) Current situation of products/services provided by deposit-taking institutions and misusing cases

Classifying transactions misused for ML over the past three years by type of products or services, products and services provided by deposit-taking institutions account for the largest share.

(a) Deposit/savings accounts

a Current situation

Based on the reliability of deposit-taking institutions and the fulfillment of a deposit protection system for depositors, deposit/savings accounts are a popular and widespread way to manage funds safely and securely. In recent years, it is possible for customers to open an account or transact through the Internet without physically visiting a bank, and deposit-taking institutions that provide services only over the Internet are becoming popular, making it increasingly convenient.

On the other hand, characteristics such as the extensiveness of savings deposit/savings accounts being widespread, are vulnerabilities for products and services. In addition, non-face-to-face transactions make it easy to impersonate a third party. Therefore, deposit/savings accounts that can be opened and used non-face-to-face can be an effective means for those intending to commit ML/TF to receive and conceal criminal proceeds.

The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct verification at the time of transactions and prepare and preserve verification records and transaction records when they conclude deposit/savings agreements (agreements for the receipt of deposit/savings) with customers.

The Act on Damage Recovery Benefit Distributed from Fund in Bank Accounts Used for Crimes requires deposit-taking institutions to take proper measures against a deposit account, such as by suspending a transaction related to it when there is suspicion about the deposit account being misused for crime, e.g., online and telephone fraud, based on information provided by investigative agencies or others about that account.

b Typologies

The following cases are common examples of misusing deposit/savings accounts for ML:

- Offenders used accounts belonging to other parties including foreigners who have returned to their home countries or deceased persons, and without following procedures to close the accounts, deposited criminal proceeds from fraud and theft.

---

*[1] The financial sector analysis conducted by the Financial Services Agency is a framework for classifying financial institutions into sectors and identifying and assessing the risks of each classification, and is the basis for inspections and monitoring based on a risk-based approach. In identifying and assessing risks, in addition to the NRA-FUR, information collected through inspections and monitoring by the Financial Services Agency, etc., as well as publicly available information, are utilized. Moreover, by taking into account the products/services provided in each sector, the transaction types, and other sector-specific risk factors, the vulnerabilities of each sector are analyzed. In addition, a relative comparison of the size of risks between business types is made, taking into account the number of STRs included in the NRA-FUR.

- Offenders used accounts sold for the purpose of obtaining money, accounts opened under fictitious or other parties' names, and accounts illegally opened in the name of shell companies to deposit criminal proceeds derived from fraud, theft, loan-shark crime, offences related to adult entertainment business, drug-related offences, and counterfeit goods offences.
- Criminal proceeds obtained through violations of the Copyright Act (Act No. 48 of 1970), specifically by uploading multiple manga titles to the Internet without the authorization of the copyright holders, were deposited into foreign bank accounts and other accounts.

In these cases, fictitious or third-party bank accounts were frequently used as a means of concealing criminal proceeds. Some instances involved the misuse of thousands of such accounts, and in certain cases, hundreds of passbooks and cash cards were seized from operational bases. These accounts have become major tools for ML/TF.

Most misused accounts are those under the names of individuals and included accounts borrowed from a family member or friend, accounts purchased from a third party, and accounts illicitly transferred from resident foreigners returning to their home countries. In recent years, it has been confirmed that criminal groups are soliciting account trafficking through social media. Looking at the trends by type of offences, there is a tendency that accounts under the names of debtors are used for loan-shark crimes; accounts under the names of relatives or acquaintances of Boryokudan members are used for gambling crimes; and accounts under the names of fictitious or other parties are used for online and telephone fraud and investment/romance fraud via social media.

There have also been confirmed cases where accounts in corporate names are misused to receive large amounts of proceeds from organized crime in online and telephone fraud or cross-border ML offences.

(b) Deposit Transactions

a Current situation

With the spread of ATMs in convenience stores, etc. deposit-taking institutions offer people great convenience by allowing them to withdraw and deposit funds (hereinafter referred to as "deposit transactions") quickly and easily, regardless of the time and place.

On the other hand, persons who intend to commit ML/TF may exploit the safety and reliability of account-based fund management, as well as the high convenience of deposit transactions, to carry out ML/TF by withdrawing proceeds transferred to accounts or depositing proceeds they have obtained. In online and telephone fraud cases, deposit transactions are actually misused for ML. For example, a crime group made victims, including elderly people, transfer money from their deposit/savings accounts to the deposit/savings accounts of fictitious or other parties' name used by the crime group to withdraw money.

The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct verification at the time of transactions, and prepare and preserve verification records and transaction records when they conduct transactions with customers that involve the receipt or payment of cash exceeding 2 million yen (100,000 yen in the case of exchange transactions or issuing a cashier's check).

b Typologies

The following cases are common examples of misusing deposit transactions for ML:

- An offender withdrew cash that were proceeds derived from fraud conducted abroad and transferred to an account in Japan by disguising them as legitimate business proceeds, by giving false explanations for the reason, such as “car export proceeds.”
- An offender deposited criminal proceeds obtained from theft, fraud, loan-shark crimes, drug crimes, and gambling into accounts opened in fictitious or other parties’ names.
- An offender deposited cash obtained through theft into the account of a relative using an ATM immediately after committing a crime, for fear of being found out to be in possession of the cash.
- An offender deposited some of the cash obtained through robbery into an account in multiple transactions within a short period under the name of an acquaintance via an ATM.
- An offender sold items obtained through theft, had the proceeds transferred to an account managed by the offender themselves, and then, at a bank counter, gave a false reason for the withdrawal, such as buying a friend’s car with cash, and withdrew the cash, under the guise of a legitimate deposit transaction.

(c) Domestic Exchange Transactions

a Current situation

Domestic exchange transactions are used for receiving remittances of salaries, pensions, dividends, etc., or for paying utility fees, credit card charges, etc., via an account transfer system. Domestic exchange transactions enable customers to make secure and quick settlements without moving physical cash from one place to another. The spread of ATMs and Internet banking has made domestic exchange transactions widely used as a familiar settlement service.

On the other hand, the transferability of domestic exchange transactions, the characteristics which allow funds to be transferred easily, quickly, and over a wide area, also constitutes one factor contributing to the vulnerability of domestic exchange transactions. Furthermore, anonymity can also be ensured by using non-face-to-face transactions such as online banking and accounts under the names of fictitious or other parties. Therefore, domestic exchange transactions can be an effective means for ML/TF.

The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct verification at the time of transactions and to prepare and preserve verification records and transaction records for exchange transactions when they receive or pay cash that exceeds 100,000 yen to customers. In addition, in the case of domestic exchange transactions involving the payment of funds to other financial institutions, when the receiving financial institutions request the paying financial institutions to conduct customer identification related to the transactions, the Act on Prevention of Transfer of Criminal Proceeds requires the paying financial institutions to prepare records on matters that enable the search of customers’ records to be verified within three business days of the request date, and requires the receiving financial institutions to prepare records concerning matters that enable the search of information concerning transactions.

b Typologies

The following are examples of cases in which domestic exchange transactions have been misused for ML:

- An offender sold fake brand goods by cash on delivery, and had a courier company transfer payments from customers to an account under the name of fictitious or other party managed by the suspect, through a third-party business operator who did not know the situation.
- An offender used account information of customer's online brokerage accounts illegally obtained in the course of their business and had the deposit money from that customer's account transferred to an account in the customer's name that the suspect had fraudulently opened and managed.
- An offender dispatched illegally overstayed foreigners in Japan as workers, and had the compensation transferred in multiple installments from the receiving company to an account in the name of the offender's acquaintance managed by the suspect.
- An offender had funds transferred from a corporate account, managed by the offender in the course of business, to an unsuspecting acquaintance's account as fictitious salary payments, by requesting to a financial institution, and then had the funds further transferred from that acquaintance's account to the suspect's account.
- An offender who was operating a money lending business without registration had repayment money from several thousand customers transferred to multiple accounts under the names of fictitious or other parties controlled by the suspect.

Domestic exchange transactions are considered one of the transaction types susceptible to ML, because non-face-to-face transactions, such as online banking, and the use of fictitious or third-party accounts make it possible to ensure anonymity.

(d) Safe-Deposit Box

a Current situation

A safe-deposit box is a service that involves a lease of a depository. While anyone can operate safe-deposit box businesses, in reality, the service most widely used is that in which deposit-taking institutions, such as banks, lease out storage space set up within their branches for a profit.

Safe-deposit boxes of deposit-taking institutions are generally intended for storing valuables and important documents, such as securities, bankbooks, bonds, deeds, or property, such as precious metals and stones. However, under the terms of the contract, deposit-taking institutions do not inspect the contents of items stored in safe-deposit boxes on a case-by-case basis, and the contents are, in principle, known only to the user. As a result, safe-deposit boxes offer a very high level of confidentiality, and there have been cases where criminal proceeds from copyright infringement or loan sharking, as well as cash, gold bars, and other valuables, were illegally stored. In recent years, there have also been incidents where employees of deposit-taking institutions have stolen cash or gold bars kept in users' safe-deposit boxes.

As such, because safe-deposit boxes combine opaqueness of stored contents with a high degree of confidentiality, they can potentially be misused by individuals intending to engage in ML/TF. In May 2025, the Financial Services Agency revised comprehensive supervisory guidelines for major banks and other deposit-taking institutions to ensure the proper conduct of safe-deposit box operations. Based on these supervisory guidelines, deposit-taking institutions have implemented measures such as excluding items considered high-risk from being stored in safe-deposit boxes and establishing internal management systems to ensure proper administration of safe-deposit boxes, from the perspective of preventing ML and misuse. In June 2025, the Japanese Bankers Association also revised its guidelines for member banks and announced a policy of not accepting cash deposits in safe-deposit boxes.

In addition, The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct verification at the time of transactions, and prepare and preserve verification records and transaction records when they make lease contracts for safe-deposit boxes with customers.

b Typologies

The following are examples of cases of misusing safe deposit boxes for ML:

- An offender cheated a victim out of their promissory note, converted it to cash, and preserved a portion of the cash in a safe deposit box that was leased from a bank by a relative.
- Criminal proceeds from fraud were offered to Boryokudan and stored by a senior member of the Boryokudan in a safe deposit box that had been registered in the name of one of his family members.

In addition, it has been confirmed that safe deposit boxes registered in the name of other persons have been used as a means of physically concealing criminal proceeds.

(e) Bills and Checks

a Current situation

Bills and checks have traditionally been widely used in Japan as a means of payment substituting for cash, owing to their high credibility with clearing systems or settlement functions provided through deposit-taking institutions. As paper-based instruments, bills and checks are physically lighter and easier to transport than cash, and can be easily transferred through endorsement, giving them high transferability. Another notable characteristic is that they could be quickly converted into cash through deposit-taking institutions.

Such high portability, transferability, and convertibility can also constitute vulnerabilities as products or services, creating a risk that they may be used as means for the physical transfer or concealment of criminal proceeds, or for disguising them as legitimate funds.

On the other hand, with regard to bills and checks, the government has called on the industry to abolish their use, citing reasons such as the time required for settlement and the potential to adversely affect the cash flow of recipient companies. In 2022, paper-based bill clearing houses nationwide were abolished, and the operation of the electronic clearing house is also scheduled to be discontinued at the end of fiscal year 2026. As a result, from fiscal year 2027 onward, settlements by bills or checks are expected to require the physical delivery of the instruments between financial institutions on an individual basis, and their practical use is therefore anticipated to become significantly limited in the future.

The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct verification at the time of transactions, and prepare and preserve verification records and transaction records when they make bill discount contracts and when they carry out transactions that receive and pay unlined bearer checks or checks drawn to self that exceed 2 million yen and are not crossed (in the cases where cash receipt and payment is involved and related to exchange transactions or checks drawn to self, 100,000 yen).

b Typologies

The following are examples of cases of misusing bills and checks for ML:

- An illegal money-lending business operator made many borrowers draw and send checks, etc. by post under the pretext of payment of principal and interest. The funds were then, through the collection process, transferred to accounts opened in the name of fictitious or other party.
- With respect to promissory notes that were defrauded from business partners under the pretense of legitimate commercial transactions, an offender forged delivery notes and invoices from fictitious suppliers during accounting procedures, in order to make it appear that the criminal proceeds were legitimate business earnings.

[Threats and Vulnerabilities Found by Competent Authorities in Recent Years]

- It was found in the payment and collection agency scheme that there are business operators that obtain the ‘rights to receive payments on behalf of other business operators located abroad and receive deposits at a bank account opened by themselves from third parties who intend to transfer funds to the said other business operators, and send collected funds in bulk (so-called “bulk remittance”) to the said other business operators. There is a risk for banks, the same as for funds transfer service providers, that they cannot verify the identity of persons sending money to customers or persons who eventually receive funds.
- The number of phishing emails sent to an unspecified large number of recipients, impersonating JA Bank and similar institutions, remains at a high level.
- There are cases in which ML is carried out using active corporate accounts, and by commingling criminal proceeds with legitimate business earnings, there is a risk that the origin of the criminal proceeds becomes obscured.
- There have been repeated instances of improper enforcement proceedings attempting to withdraw funds from accounts that had been frozen on suspicion of criminal misuse, using documents such as payment orders issued by courts or notarized deeds prepared by notaries based on false claims.

(ii) Trends of STRs

The number of STRs submitted by deposit-taking institutions from 2022 to 2024 is as follows:

Table 73: The Number of STRs Submitted by Deposit-taking Institutions

Category / Year	2022	2023	2024	Total
Deposit-taking Institution (cases)	435,728	522,649	611,069	1,569,446

The Financial Services Agency revised the “List of Reference Cases of Suspicious Transactions” for deposit-taking institutions by adding reference cases that focus on abnormal transactions specific to Internet-based transactions and financing of terrorism, and released it in August 2025.

The reasons for submitting reports (guideline numbers and names in the “The guideline numbers and names in Guidance for Submitting STRs” [*1]) that recorded the highest number of reports between 2022 and 2024 are as follows.

[*1] “The guideline numbers and names in Guidance for Submitting STRs, 9th edition” by the National Police Agency (revised August 2025).

Table 74: Reporting Status of Major STRs by Deposit-taking Institutions[*1*2]

Reason for report	Number of reports (cases)	Percentage (%)
43. Customers with unusual behavior or movements	430,057	27.4
14. Frequent remittances from numerous individuals	150,203	9.6
42. Transactions related to Boryokudan gangsters or their related parties	113,702	7.2
27. Large remittances from/to other countries for economically unreasonable purposes	84,893	5.4
16. Sudden large deposits, withdrawals and remittances	76,716	4.9
44. Unusual transactions based on the purpose, occupation or content of business	67,525	4.3
1. Large cash transactions	66,182	4.2
11. Frequent large deposits, withdrawals and remittances	65,006	4.1
13. Frequent remittances from numerous individuals	47,470	3.0
5. Transactions under fictitious or other party’s name	47,004	3.0

Furthermore, various deposit-taking institutions, including banks that provide services only on the Internet, have submitted STRs focusing on customers’ IP addresses and mobile phone numbers.

The details of transactions that are suspected to be made with fictitious or borrowed names are as follows:

- Headshots attached to the principal identification documents of several users with different names and dates of birth were identical
- More than one account opening or user registration was made from the same IP address
- The country of residence of a user was Japan, but the IP address assigned at the time of login was allocated outside Japan
- The same mobile phone number was registered as the contact for more than one account or user, but the phone number was not in use
- Taking into account customer attributes such as residence and occupation, it appears unnatural for customers to open accounts at the respective deposit-taking institution or branch. Additionally, similar applications occur simultaneously.

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, each relevant law and regulation contains on measures to mitigate risks.

○ Act on Prevention of Transfer of Criminal Proceeds

[*1] Showing the number of submitted STRs and their percentages by reason for report for the period from 2022 to 2024 (the same applies to the following business operators).

[*2] Among the guideline numbers and names, “Inquiries from public institutions regarding criminal proceeds” and “Other” are excluded from the “Reporting Status of Major STRs” tables (this also applies to the businesses types described hereafter).

Stipulates that specified business operators are obligated to perform customer verification and other measures at the time of transactions. It also stipulates that specified business operators must notify other specified businesses operators or foreign-exchange transaction operators when conducting foreign exchange transactions of information about customers and the recipients of payments.

○ Banking Act

Stipulates that the Financial Services Agency has the right to collect reports from, conduct on-site inspection of, and issue improvement orders against banks as necessary.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision for Major Banks	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision for Small, Medium-Sized, and Local Financial Institutions	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision for Agricultural Cooperative Credit Business	https://www.maff.go.jp/j/keiei/sosiki/kyosoka/k_sido/ (Ministry of Agriculture, Forestry and Fisheries)
Comprehensive Guidelines for Supervision for Fishery Cooperative Credit Business	https://www.jfa.maff.go.jp/j/keiei/gyokyou/sisin/ (Fisheries Agency)

[Examples of Initiatives Taken by Competent Authorities]

<Financial Services Agency>

- Promoting the holding of cross-industry forums themed on "Measures Against Fraudulent Use of Bank Accounts" based on the request letter jointly issued in August 2024 with the National Police Agency. Strengthening coordinated regional efforts through the sharing of case studies and initiatives related to financial crime countermeasures, as well as the conclusion of cooperation agreements between prefectural police and financial institutions.
- In response to evolving ML/TF risks, published the "Issues and practices for dialogue on validation of effectiveness of AML/CFT frameworks," which sets out concepts and approaches for validating effectiveness in order to maintain and enhance the frameworks established in accordance with the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (March 2025).
- Revised the Comprehensive Supervisory Guidelines for Major Banks and Other Institutions, as well as the Comprehensive Supervisory Guidelines for Small and Medium-Sized and Regional Financial Institutions, from the perspective of securing the effectiveness of measures to prevent ML/TF to ensure the proper management of safe-deposit box services by financial institutions (May 2025).

<Ministry of Agriculture, Forestry and Fisheries>

- Conducted exchanges of views on the actual state of AML/CFT measures with the Prefectural Credit Federations of Agricultural Cooperatives and the Prefectural Credit Federations of Fisheries Cooperatives, which serve as supervisory bodies for agricultural and fisheries cooperatives, as well as with the prefectural governments that have jurisdiction over such cooperatives (From July to December 2024).
- Held an exchange of views with the management of the Norinchukin Bank, the central institution of the cooperative financial system, and shared awareness of issues related to ML countermeasures, including the fraudulent use of bank accounts (January 2025).
- Issued a joint notice with the Financial Services Agency and the National Police Agency to the Norinchukin Bank and each prefecture to ensure that measures at cooperative financial institutions are effectively implemented, and requested that cooperative financial institutions strengthen their efforts to prevent the fraudulent use of bank accounts in light of requests from the Financial Services Agency and the National Police Agency (January 2025).
- Held briefing sessions for the Prefectural Credit Federations of Agricultural and Fisheries Cooperatives and for prefectural governments, sharing a sense of urgency regarding ML and requesting appropriate guidance (January 2025).
- Requested reports from agricultural and fisheries cooperatives on the actual status of their credit business transactions and their organizational frameworks, and conducted risk analyses based on the submitted reports.
- Conducted inspections of agricultural and fisheries cooperatives and related entities to verify their compliance with the Guidelines (from April 2024 to March 2025: 12 Prefectural Credit Federations of Agricultural Cooperatives, 4 Prefectural Credit Federations of Fisheries Cooperatives, and 16 agricultural cooperatives at the request of prefectural governments)

<Ministry of Health, Labour, and Welfare>

- Conducted targeted AML inspections (two cases in 2024 and two cases in 2025) and supervisory activities in coordination with the Financial Services Agency and the Local Finance Bureaus with respect to labour banks.
- Held a briefing and exchange of views with the management and other senior officials of labour banks regarding AML/CFT measures in coordination with the Financial Services Agency (August 2024)

The Financial Services Agency has requested financial institutions, including those handling deposits, to complete the improvement of their management framework by March 2024, in accordance with the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism” revised in February 2021. The Financial Services Agency has received reports from most of the financial institutions that they have completed establishing their management framework, and the Agency has evaluated that the intensive efforts have achieved a certain effect. As it is now necessary for financial institutions to advance their risk-based approaches and move on to a stage of maintaining and enhancing the effective management frameworks, the Financial Services Agency published in March 2025 the “Issues and practices for dialogue on validation of effectiveness of AML/CFT frameworks,” which outlines concepts and approaches for validating effectiveness. The Financial Services Agency will monitor the status of these validation efforts and will work to implement and promote effectiveness validation at financial institutions and other organizations.

In addition, in August 2024, the Financial Services Agency and the National Police Agency jointly requested industry associations to take the various measures to prevent the illicit use of deposit/savings accounts. Furthermore, in light of the increasingly sophisticated and diverse criminal methods, combined with the misuse of online banking, there have been cases in which funds obtained through online and telephone fraud and similar schemes were transferred to the bank accounts of cryptoassets exchange service providers or funds transfer service providers. Accordingly, in September 2025, the authorities issued a request for measures that included the contents of the previous request from August 2024, as follows:

(1) Strengthening fraud prevention measures and improving understanding of customer circumstances at the time of account opening

(2) Multi-layered detection focusing on appropriateness of user's access environment and the amount and frequency of transactions

(3) Enhancing and refining detection scenarios and thresholds focusing based on the purpose of illicit use and the modus operandi

(4) Expediting detection and subsequent confirmation with customers, as well as measures such as suspension of withdrawals, freezing of accounts, and account closure

(5) Strengthening measures related to online banking

- Verification and warnings at the time of application
- Appropriate setting of initial usage limits
- Verification and warnings after service commencement and when raising usage limits

(6) Suspension of transfers to cryptoassets exchange service providers and funds transfer service providers when the remitter name has been altered

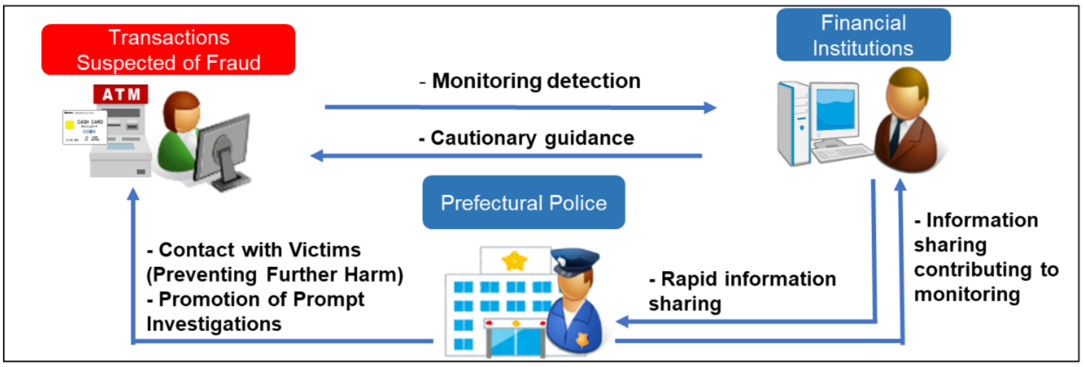
(7) Information sharing among financial institutions that contributes to detecting signs of illicit activity and the understanding the actual situation.

(8) Strengthening information provision and cooperation with the police

These requests reflect the worsening situation of financial crimes, such as non-face-to-face fraud and the fraudulent use of corporate accounts, and call for the prompt implementation of effective countermeasures.

Regarding (8) "Strengthening information provision and cooperation with the police," as of the end of September 2025, the National Police Agency has concluded information-sharing agreements with 28 financial institutions. These agreements provide for the rapid sharing with the relevant prefectural police and the National Police Agency of information concerning accounts related to transactions identified through monitoring by financial institutions as having a high risk of fraud. Additionally, as of the end of June 2025, 44 prefectural police have established cooperation with 515 financial institutions.

Table 75: Illustration of Information Sharing Between the Police and Financial Institutions



In addition, as part of the “measures to deprive criminals of their tools” outlined in the “Comprehensive Measures to Protect People from Frauds” formulated in June 2024, the National Police Agency issued in December 2024 a notification to the relevant government ministries overseeing financial institutions, requesting that the following specific measures be implemented at each financial institution to prevent the misuse of deposit accounts held in the names of foreigners whose period of stay has expired:

- When cash withdrawals or transfers to other accounts are made from an account held by a foreigner whose period of stay has expired, conduct verification at the time of transaction to confirm that the account is being used by the account holder in person
- From the day after the expiration of the residency period, until such verification is completed, restrict cash withdrawals and transfers to other accounts from the relevant account[*1*2]

(C) Measures by industry associations and business operators

Industry associations support the AML/CFT measures of each deposit-taking institution by providing case examples, supplying a database on people whose assets are to be frozen, and offering training. Deposit-taking institutions themselves are endeavoring to establish and reinforce their own AML/CFT internal control systems too. For example, they set up a division in charge, develop internal regulations and manuals, carry out periodic trainings, conduct internal audits, screen out transactions that are likely to have higher risks, and adopt enhanced monitoring for transactions with higher risks.

Furthermore, as part of efforts to enhance and streamline core AML/CFT operations at financial institutions, such as transaction monitoring, the licensed foreign exchange transaction analysis business, established following the amendment to the Payment Services Act (enforced on June 1, 2023), has been launched[*3].

Furthermore, the Japanese Bankers Association is advancing discussions on establishing a system for sharing information on fraudulently used accounts among financial institutions, as a measure against online and telephone fraud, investment/romance fraud via social media, and similar schemes. This is expected to strengthen AML/CFT through rapid and reliable information sharing.

[Examples of Initiatives Taken by Industry Associations and Specified Business Operators][*4]

<Industry Association>

- Each industry association created a document that organizes the key points and standards for establishing the internal control framework required by the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism” and the “Frequently Asked Questions Regarding ‘Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism’ (FAQ),” and distributed it to all members (Regional Banks Association of Japan, Second Association of Regional Banks, National Association of Shinkin Banks, National Central Society of Credit Cooperatives, National Association of Labour Banks)

[*1] Deposits (including deposits via bank transfer), automatic withdrawals, and automatic transfers are not subject to these restrictions.
[*2] If, after the restriction, the account holder presents a residence card at the branch or otherwise confirms the renewal of the residency period, the restriction will be lifted, allowing normal transactions to resume.
[*3] Information on the licensed foreign exchange transaction analysis business is described in the 2024 Survey Report, “[Topic] Joint Transaction Monitoring by Financial Institutions” (page 119).
[*4] In “Examples of Initiatives Taken by Industry Associations and Specified Business Operators” and “Examples of Initiatives Taken by Industry Associations,” the type of legal entity in the name of the industry association is omitted.

● A study session was held by the representative bank to introduce its initiatives (Regional Banks Association of Japan, Second Association of Regional Banks)

● In response to partial revisions to the supervisory guidelines on safe deposit box operations, the model safe deposit box regulations were revised and sample declaration forms for verifying the purpose of use, etc. were prepared (the Japanese Bankers Association).

● Regarding the establishment of risk management frameworks for ML/TF, verification by external experts was conducted and a briefing session for all labour banks was held in December 2024 to present the verification results and potential issues (the Labour Banks' Federation).

● In June and December 2024, exchange meetings among labour banks were held, where questions collected in advance from other banks, responses, and notable initiatives were shared within the sector (the Labour Banks' Federation).

● By the end of March 2024, system and regulatory framework enhancements were implemented. Going forward, the bank plans to use these systems to investigate and analyze customer attributes with a high risk of fraudulent use and to verify the effectiveness of countermeasures (Norinchukin Bank).

● In response to requests from the Financial Services Agency and the National Police Agency, Norinchukin Bank urged its affiliated cooperative financial institutions to strengthen measures to prevent the fraudulent use of accounts, and simultaneously conducted a comprehensive review of financial crime countermeasures within JA Bank (Norinchukin Bank).

● A dedicated department for financial crimes and ML has been established, promoting AML/CFT measures such as monitoring the implementation status at agricultural cooperatives (Norinchukin Bank).

● In certain prefectural areas, efforts to share information through cooperation agreements with prefectural police are progressing (Credit Federations of Agricultural Cooperatives).

● Identity re-verification surveys were conducted and a "National Briefing on Measures Against Money Laundering and Terrorist Financing" was held for its affiliated cooperative financial institutions (Norinchukin Bank).

<Specified Business Operators>

● Due to the detection of multiple instances involving the deposit of criminal proceeds from online and telephone fraud or unauthorized transfers into dedicated deposit accounts, followed by the purchase and immediate withdrawal of cryptoassets, some deposit-taking institutions have taken measures to verify the ML/TF risk management capabilities of cryptoassets exchange service providers. These measures include issuing questionnaires and providing the capability for cryptoassets exchange service providers to suspend the use of dedicated deposit accounts in cases of detected misuse.

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, the key matters that deposit-taking institutions should continue to consider for AML/CFT measures are as follows:

- Comprehensively and specifically identify ML/TF risks.
- Go beyond mere compliance with laws such as the Act on Prevention of Transfer of Criminal Proceeds and conduct CDD commensurate with the risk.
- Utilize the foundational framework established by the end of March 2024 and ensure its maintenance and further enhancement by implementing the PDCA cycle.
- To prevent the fraudulent use of deposit/savings accounts, including corporate accounts, analyze the modus operandi of fraudulent activities, such as criminal methods and access environments, and strengthen countermeasures accordingly.

(v) Assessment of Risks

Deposit-taking institutions provide various products and services, including accounts that guarantee safe fund management, deposit transactions for easy preparation or storage of funds regardless of time and place, exchange transactions for transferring funds from one place to another or many people quickly and securely, safe-deposit boxes for safe storage of property while maintaining secrecy, and bills and checks that are negotiable and easy to transfer.

These same characteristics of financial products and services can make them convenient for transferring criminal proceeds. There are cases where financial products and services have been misused to receive or conceal criminal proceeds. As such, it is recognized that products and services of deposit-taking institutions present risks of misuse for ML/TF.[*1*2]

Furthermore, based on the status and role of Japan as an international financial market, the large financial transaction volume of the industry as a whole, figures in the statistics of transactions misused for ML/TF, cases where cross-border crime organizations are involved, and recent criminal environment, the risk of misuse for ML/TF is considered to be relatively high in comparison with other types of businesses.

In addition, in light of cases where products or services provided by deposit-taking institutions were misused for ML, it is recognized that the following transactions are at a higher risk in addition to those described in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attribute:*

- Transactions under anonymous or fictitious and borrowed names (including suspected ones)
- Transactions made by numerous people
- Frequent transactions
- Transactions involving large amounts of remittances and deposits or withdrawals
- Transactions where sudden large deposits and withdrawals are made in accounts that normally do not move funds
- Transactions involving remittances, deposits, and withdrawals performed in an unnatural manner and frequency in light of the purpose of the account holders’ transactions, occupations, and business contents
- Transactions involving deposits and withdrawals using the accounts of customers who have multiple accounts (including accounts held under different names using store names)

Competent authorities and specified business operators are taking the aforementioned mitigating measures against these risks, and the outcomes of such measures can be seen from the effective efforts made by deposit-taking institutions.

However, these efforts differ from one deposit-taking institution to another. Deposit-taking institutions that are

[*1] Article 2, paragraph (2), item (xxviii) of the Act on Prevention of Transfer of Criminal Proceeds provides that mutual loan companies are specified business operators. In a mutual loan, a mutual loan company sets a certain number of units, and benefits are paid periodically, clients regularly pay premiums, and they receive property other than cash through lotteries, bids, etc. for each unit. Mutual loans have a characteristic that is similar to deposits in terms of the system of premiums and benefits, so it is recognized that they carry the risk of being misused for the transfer of criminal proceeds.

[*2] Article 2, paragraph (2), item (xxxvi) of the Act on Prevention of Transfer of Criminal Proceeds provides that electronic monetary claim recording institutions are specified business operators. Electronically recorded monetary claims are made or transferred by electronically recording them in registries created by electronic monetary claim recording institutions on magnetic disks or the like. Electronically recorded monetary claims function similarly to bills in terms of smooth assignment receivables, so it is recognized that they carry the risk of being misused for the transfer of criminal proceeds.

not taking effective risk-mitigating measures corresponding to their risks may face a greater risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

In particular, in light of the situation in which accounts under the names of fictitious or other parties are being misused, as described in this section and in “Section 3 1. Offenders” of this NRA-FUR, deposit-taking institutions that offer accounts are required to implement continuous measures to prevent the transfer of accounts and to detect fraudulent transactions after the fact.

[Electronic Payment Handling Service Providers[*1]*]*

Amidst the increasing digitalization of the overall economy, digitalization is also accelerating in the financial sector, including the utilization of distributed ledger technology. This has led to changes in the products and services offered by deposit-taking institutions such as banks. In light of these developments, to promote private-sector innovation and ensure appropriate user protection, a law amending certain provisions of the Payment Services Act and other related laws was enacted in June 2022 (Act No. 61 of 2022; hereinafter referred to as the “Amendment Act to the Payment Services Act”). This amendment to laws, including the Banking Act*[2], introduces regulatory measures such as registration requirements for electronic payment handling services. Electronic payment handling services were added as specific business operators under the Act on Prevention of Transfer of Criminal Proceeds through amendments to the said Act.

Electronic payment handling service providers operate businesses that, on behalf of banks etc., use electronic data processing systems to transfer funds in accounts, reduce the volume of deposit claims equivalent to the transferred funds, or increase the volume of deposit claims equivalent to the funds received through exchange transactions with depositors who have opened deposit accounts with banks, etc.

Due to being added to the list of specific business operators under the Act on Prevention of Transfer of Criminal Proceeds, electronic payment handling service providers are subject to various obligations under this Act, including conducting verification at the time of transactions, preparing and preserving verification records, and submitting STRs. Additionally, they are prohibited from accepting deposits of funds from users. Furthermore, the users of electronic payment handling service providers are limited to depositors with the respective banks, and various risk mitigation measures by deposit-taking institutions have also been put in place. As a result, the risk of ML/TF is considered to be mitigated to a level comparable to the services provided by deposit-taking institutions.

*1 Electronic payment handling service providers, electronic payment handling services for Shinkin Banks, and electronic payment handling services for Credit Cooperatives

*2 The Banking Act, the Shinkin Bank Act (Act No. 238 of 1951) and the Act on Financial Business by Cooperatives (Act No. 183 of 1949).

(2) Insurance Dealt with by Insurance Companies, etc.

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Basically, insurance contracts represent a promise to pay insurance benefits in connection with the life or death of individuals or a promise to compensate for losses caused by a certain incident. Payment is limited to cases where those conditions, which have uncertainty, are met. This characteristic significantly mitigates the risks of insurance carries being misused for ML/TF.

However, each insurance product varies in regard to its characteristics. Insurance companies[*1] provide some products that have cash accumulation features. Unlike insurance products that provide benefits based on future accidents, some products with cash accumulation features provide benefits based on conditions that are more certain to be met, such as policies with a maturity benefit. These products may, in many cases, provide a considerable amount of cash surrender value when contracts are canceled before maturity. For example, if an insurance premium is paid at the time of concluding a contract and then the contract is canceled promptly, the risk is particularly high. It also should be noted that the risk of being misused for ML/TF is particularly high in cases where the premium allocation amount is refunded due to the cooling off.

This characteristic of the convertibility of the source funds into insurance products (or from insurance products to other asset forms) is a vulnerability for products and services and can be misused for ML/TF.

As of the end of March 2025, 98 insurance companies etc. had obtained a license from the Prime Minister based on the Insurance Business Act (Act No. 105 of 1995). In addition, there are small-amount and short-term insurance companies registered by the Prime Minister and agricultural cooperatives established with a permit given by the Minister of Agriculture, Forestry and Fisheries.

In its financial sector analysis, the Financial Services Agency has assessed the sector risk of insurance as “Low,” which means relatively low.

(B) Typologies

The following case is an example of cases where insurance products were misused for ML and criminal proceeds were transformed:

- Criminal proceeds derived from fraud and prostitution were spent on the purchase of installment life insurance for offenders and their family members.

The following case is an example of insurance related to ML:

- An offender stole non-life insurance money for losses for missed work derived from fraud by making an insurance company transfer the money to an account in fictitious or other party’s name.

(ii) Trends of STRs

The number of STRs submitted by insurance companies from 2022 to 2024 is as follows:

[*1] Insurance companies, etc. mean those listed in Article 2, paragraph (2), item (viii) (agricultural cooperatives), item (ix) (federations of agricultural cooperatives), item (xvii) (insurance companies), item (xviii) (foreign insurance companies, etc.), item (xix) (small-claim/short-term insurance business operators), and item (xx) (mutual aid insurance federation of fishery industry cooperatives) of the Act on Prevention of Transfer of Criminal Proceeds.

Table 76: The Number of STRs Submitted by Insurance Companies

Category / Year	2022	2023	2024	Total
Life Insurance (cases)	3,521	4,029	4,814	12,364
General Insurance (cases)	407	532	603	1,542
Mutual Aid (cases)	11	12	4	27

The Financial Services Agency revised *the List of Reference Cases of Suspicious Transactions* for insurance companies by adding reference cases focused on abnormal transactions specific to Internet-based transactions and financing of terrorism, and released it in March 2022.

The reasons for submitting reports (guideline numbers and names in the "The guideline numbers and names in Guidance for Submitting STRs") that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 77: Reporting Status of Major STRs by Life Insurance

Reason for report	Number of reports	Percentage (%)
28. Transactions related to Boryokudan gangsters or their related parties	6,831	55.2
29. Customers with unusual behavior or movements	600	4.9
2. Payment of large insurance claims in cash	310	2.5
11. Economically unreasonable transaction	278	2.2
3. Frequent in a short-term, with large total amount of cash	69	0.6

Table 78: Reporting Status of Major STRs by General Insurance

Reason for report	Number of reports	Percentage (%)
28. Transactions related to Boryokudan gangsters or their related parties	562	36.4
29. Customers with unusual behavior or movements	78	5.1
11. Economically unreasonable transaction	22	1.4
5. Transactions under fictitious or other party's name	2	0.1

Table 79: Reporting Status of Major STRs by Mutual Aid

Reason for report	Number of reports	Percentage (%)
28. Transactions related to Boryokudan gangsters or their related parties	27	100

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transaction, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Insurance Business Act

Stipulates that the competent authorities have the right to issue an order to submit reports, conduct on-site inspections, and issue improvement orders, as necessary.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision for Insurance Companies	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Guidelines for Supervision for Small-Amount and Short-Term Insurance Companies	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision for Authorized Specified Insurers	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision for Agricultural Cooperative Mutual Aid Business	https://www.maff.go.jp/j/keiei/sosiki/kyosoka/k_sido/ (Ministry of Agriculture, Forestry and Fisheries)
Comprehensive Guidelines for Supervision for Fishery Cooperative Mutual Aid Business	https://www.jfa.maff.go.jp/j/keiei/gyokyou/sisin/ (Fisheries Agency)

[Examples of Initiatives Taken by Competent Authorities]

<Financial Services Agency>

- Provided lectures and training to other ministries and agencies, industry associations, specified business operators and foreign authorities insurance officers to improve AML/CFT.
- Published the "Issues and practices for dialogue on validation of effectiveness of AML/CFT frameworks," which sets out concepts and approaches for validating effectiveness in order to maintain and enhance the frameworks established in accordance with the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism," in response to evolving ML/TF risks (March 2025)

<Ministry of Agriculture, Forestry and Fisheries>

- Requested reports from the competent organizations conducting mutual aid businesses regarding their transaction activities and the status of their framework development, and conducted risk analysis based on the submitted reports.
- Held consultations and exchanged views with the competent organizations conducting mutual aid businesses concerning AML/CFT
- Conducted inspections of agricultural and fisheries cooperatives, etc., to confirm their status of compliance with the Guidelines (April 2024 to March 2025; eight agricultural cooperatives upon request from prefectural governments)

(C) Measures by industry associations and business operators

In order to prevent insurance from being misused for wrongful fundraising, industry associations introduced a system that enables members to register the contents of their contracts and to refer to them when necessary. This system facilitates information sharing among members. When they receive an application to make a contract or for payment of insurance benefits, they can refer to the system to examine whether there are any suspicious circumstances (for example, if an insured person has several insurance contracts of the same type). Furthermore, the Association sets up a project team in-house, where the members of the team share information and exchange opinions at meetings hosted by the team. The Associations also create various materials, such as handbooks and Q&As, to support AML/CFT measures taken by members.

Insurance companies also take measures to establish and strengthen their AML/CFT internal control systems. For example, they set up a division in charge, develop internal rules and manuals, provide periodic training, conduct internal audits, screen out transactions that are considered to be at high risk, and adopt enhanced monitoring of high-risk transactions.

[Examples of Initiatives Taken by Industry Associations]

- Based on the policy for the fiscal 2024 projects, training and awareness-raising activities were conducted for agricultural cooperatives on measures, such as verification at the time of transaction and creation and preservation of verification records, using training materials and electronic manuals (National Mutual Insurance Federation of Agricultural Cooperatives).
- Implemented system checks (filtering and screening) to verify that mutual insurance contract holders are not sanctioned individuals or members of Boryokudan gangsters to prevent transactions in advance and address the exclusion of existing transactions (National Mutual Insurance Federation of Agricultural Cooperatives).
- Conducted system checks at the time of transactions involving cash transactions exceeding 2 million yen, cancellation of products with high-savings schemes, new contract cancellations, and cooling-offs (transaction monitoring) to alert agricultural cooperatives in determining the applicability of suspicious transactions (National Mutual Insurance Federation of Agricultural Cooperatives).
- Used electronic manuals to illustrate transactions with doubts of suspicious activities to agricultural cooperatives, such as unreasonable early cancellations, high-value cash transactions that are difficult to justify, and transactions with users from remote locations without reasonable reasons, and implemented careful review and transaction monitoring based on the presence or absence of reasonable reasons (National Mutual Insurance Federation of Agricultural Cooperatives).
- Based on the 2024 compliance program, worked to establish basic policies on compliance for officers and employees and to improve compliance in daily business operations. Regarding measures such as verification at the time of transaction, provided internal training and education, as well as training and awareness-raising for fishery cooperatives (National Mutual Aid Insurance Federation of Fishery Industry Cooperatives).
- Conducted a monitoring survey (examine whether cash is received and the reasons for receipt in case of cash) regarding a contract under which over 2 million yen was paid in a lump sum as mutual aid premiums, and also examined the monitoring survey during the internal audit (National Mutual Aid Insurance Federation of Fishery Industry Cooperatives)
- Instructed Fishery Cooperatives to ensure that the prescribed identity verification at the time of transaction was conducted, and the purpose and route of participation were thoroughly confirmed when non-members applied for a mutual aid contract, which, under internal regulations, is limited to friends and acquaintances of members or officers and staff ((National Mutual Aid Insurance Federation of Fishery Industry Cooperatives).

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual situation identified by the competent authorities, insurance companies, etc., should pay attention to the following matters for AML/CFT measures:

- Establish a system for verification at the time of transaction and ongoing CDD commensurate with the risks.
- When preparing and reviewing their AML/CFT Risk assessment documents, identify and assess the risks comprehensively and specifically, not only by quoting the contents of investigation documents or widely used templates, but also by considering the characteristics of the company's transactions, including the products/services, transaction types, countries/regions involved in the transactions, and customer attributes.
- Regarding IT systems, consider introducing systems or change the settings of existing systems, taking into account the risks they face according to the scale and characteristics of the company's business and transaction types.
- Establish and maintain an appropriate system for transaction filtering to detect transactions subject to sanctions according to the risks.
- Implement necessary measures such as complying with domestic and international laws and regulations concerning sanctioned transactions, and establish a framework for accurately detecting high-risk customers.

(v) Assessment of Risks

Since insurance products with cash accumulation features enable premiums to be paid using criminal proceeds, which enables the surrender of the policy mid-term and receipt of surrender benefits, or criminal proceeds to be converted to deferred assets, they can be an effective means of ML/TF.

Actually, there are cases where illegal proceeds related to violation of the Anti-Prostitution Act was used to buy insurance products with cash accumulation features. Considering this relevant situation, it is recognized that such insurance products have risks that can be misused for ML/TF.

In light of cases where insurance products were misused for ML, in addition to the transactions described in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, it is recognized that the risks of the following transactions will be further raised:

- Transactions under anonymous or fictitious, borrowed, and false names (including suspected ones)
- Transactions in which an insurance premium is paid when a contract is concluded, and the contract is canceled soon afterward

Competent authorities and insurance companies are taking the above-mentioned risk-mitigating measures taking these risks into account.

However, these efforts differ from one insurance company to another. Insurance companies taking ineffective risk-mitigating measures corresponding to their risks may face a greater risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(3) Products and Services Dealt with by Financial Instruments Business Operators, etc., and Commodity Derivatives Business Operators

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Besides deposits in bank account at deposit-taking institutions, investing in stocks, bonds, and other financial products are also useful ways to manage funds. Investment instruments include commodity derivative transactions related to minerals and agricultural products, as well as financial products such as stocks, bonds, and beneficiary certificates of investment trusts.

As of the end of March 2025, there were 5,967 financial instrument business operators registered by the Prime Minister or those notified to the Prime Minister based on the Financial Instruments and Exchange Act[*1]. The number of commodity derivatives business operators that had obtained permission from the competent ministers (Minister of Agriculture, Forestry and Fisheries and Minister of Economy, Trade and Industry) based on the Commodities Derivatives Act (Act No. 239 of 1950) [*2] was 36.

Upon reviewing the trading conditions of stocks and commodities as investment targets in Japan, the total transaction value of stocks listed on the Tokyo Stock Exchange in 2024 was about 1,255 trillion yen in the Prime Market, about 35 trillion yen in the Standard Market, and about 34 trillion yen in the Growth Market.

For commodity derivative transactions, the trading volumes amounted to approximately 3.93 million sheets[*3] at the Tokyo Commodity Exchange and the Osaka Dojima Exchange in 2024.

Investment has different characteristics to deposit/savings; customers risk losing principal when the market price of the investment targets fluctuates. However, at the same time, they can obtain more profit than with deposit/savings if the investment succeeds.

From the perspective of the risk of abuse for ML/TF, investments have the characteristics of convertibility, which allows large amounts of money to be converted into various products by depositing funds or trading stocks or commodity derivatives, and complexity, which makes it difficult to trace criminal proceeds by investing in financial products with complex structures and making the source of the funds unclear. These characteristics are vulnerabilities for products and services.

In recent years, the expansion of securities firms, particularly those conducting internet-based trading, has made non-face-to-face account openings and transactions commonplace, increasing the risk of account openings using forged identification documents or impersonation of others. There have also been cases of unauthorized withdrawals or trading resulting from fraudulent access to online securities accounts or account takeovers, creating a risk that funds may be moved or securities traded while impersonating the legitimate account holder.

[*1] Meaning the persons listed in Article 2, paragraph (2), item (xxi) of the Act on Prevention of Transfer of Criminal Proceeds (financial instruments business operators), persons listed in item (xxii) of the same paragraph (securities finance companies), persons listed in item (xxiii) of the same paragraph (notifiers of specially permitted services), persons listed in item (xxiv) of the same paragraph (notifiers of specially permitted services for foreign investors, etc.).

[*2] Meaning the persons listed in Article 2, paragraph (2), item (xxxiii) of the Act on Prevention of Transfer of Criminal Proceeds (commodity derivatives business operators)

[*3] "Sheet" is the term for the minimum transaction unit showing transaction volume or delivery volume that constitutes the base for transactions in an exchange.

(3) Products and Services Dealt with by Financial Instruments Business Operators, etc., and Commodity Derivatives Business Operators

The Financial Services Agency states that financial instruments business operators and commodity derivatives business operators can transfer deposits from their bank accounts to securities general accounts and FX accounts, remit money from the bank accounts to designated bank accounts, transfer securities to other accounts or other companies, or deposit and withdraw cash at the teller and ATMs, and therefore, there is a risk of transferring criminal proceeds through these transactions. For example, when providing deposit and withdrawal services linked to group's bank accounts, there is a risk that the necessary confirmations will be insufficient due to the acceleration of fund transfers. Furthermore, there is a risk that insider trading will be conducted, and the funds obtained from insider trading will be combined with legal assets, or that the sale and purchase of stocks will be used to raise funds for Boryokudan. In non-face-to-face transactions, there is a risk of dealing with a fictitious person or a person impersonating another person.

Thus, while each type of transaction carries certain risks, in its financial sector analysis, the Financial Services Agency has assessed the sector risk related to investment as "Low," which means relatively low.

(B) Typologies

The following cases are common examples of products and services dealt with by financial instruments business operators and commodity derivatives business operators, as well as brokerage services for commissioned transactions on commodity markets that were misused for ML:

- An offender remitted criminal proceeds derived from fraud into the account of a securities company that was opened under a fictitious or other party's name, and the offender purchased stocks.
- An offender, after depositing criminal proceeds from robbery into an account in his/her relative's name, deposited the criminal proceeds into an FX account opened in that relative's name as clearing margins.
- An offender used part of the defrauded funds to purchase shares of a corporation in the name of an acquaintance, had the acquaintance assume the position of corporate founder, established a stock company, and had the acquaintance appointed as its representative director.
- An offender invested the criminal proceeds obtained through embezzlement in commodity derivative transactions

(ii) Trends of STRs

The number of STRs submitted by financial instruments business operators, etc. and commodity derivatives business operators from 2022 to 2024 is as follows:

Table 80: The Number of STRs Submitted by Financial Instruments Business Operators, etc. and Commodity Derivatives Business Operators

Category / Year		2022	2023	2024	Total
Financial Instruments Business Operators	(cases)	19,032	20,550	23,804	63,386
Commodity Derivatives Business Operators	(cases)	318	846	428	1,592

The Financial Services Agency, Ministry of Agriculture, Forestry and Fisheries, and Ministry of Economy, Trade and Industry have published the "List of Reference Cases of Suspicious Transactions" for financial instruments business operators and commodity derivatives business operators. This list includes reference cases that focus on the abnormal transactions specific to internet-based transactions and issues related to TF, among others.

The reasons for submitting reports (guideline numbers and names in the "The guideline numbers and names in Guidance for Submitting STRs") that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 81: Reporting Status of Major STRs by Financial Instruments Business Operators

Reason for report	Number of reports	Percentage (%)
38. Customers with unusual behavior or movements	15,009	23.7
4. Transactions under fictitious or other party's name	13,202	20.8
37. Transactions related to Boryokudan gangsters or their related parties	9,387	14.8
42. Transactions from the same IP address by different customers	1,657	2.6
39. Unusual transactions based on the purpose, occupation or content of business	1,416	2.2

Table 82: Reporting Status of Major STRs by Commodity Derivatives Business Operators

Reason for report	Number of reports	Percentage (%)
4. Transactions under fictitious or other party's name	1,216	76.4
32. Transactions in which the true beneficiary is suspicious	40	2.5
27. Transactions from the same IP address by different customers	9	0.6
26. Customers with unusual behavior or movements	7	0.4
25. Transactions related to Boryokudan gangsters or their related parties	3	0.2

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transaction, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Financial Instruments and Exchange Act and Commodities Derivatives Act

Stipulate that the competent authorities have the right to require business operators to submit reports, conduct on-site inspections, and order business operators to make business improvement if necessary.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision of Financial Instruments Business Operators	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Basic Guidelines for Supervision of Commodity Derivatives Business Operators, etc.	https://www.maff.go.jp/j/shokusan/syoutori/dealing/attach/pdf/hourei-8.pdf (Ministry of Agriculture, Forestry and Fisheries)

	https://www.meti.go.jp/policy/commerce/z00/250701sakimono-shishin.pdf (Ministry of Economy, Trade and Industry)
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Commodity Derivatives Business	https://www.maff.go.jp/j/shokusan/syoutori/dealing/attach/pdf/money-5.pdf(Ministry of Agriculture, Forestry and Fisheries) https://www.meti.go.jp/policy/commerce/f00/211019amlcft_guideline.pdf(Ministry of Economy, Trade and Industry)
Points to consider for supervision of specified joint real estate enterprises	https://www.mlit.go.jp/totikensangyo/const/1_6_bt_000263.html (Ministry of Land, Infrastructure, Transport and Tourism)

[Examples of Initiatives Taken by Competent Authorities]

<Financial Services Agency>

- Provided lectures and training to other ministries and agencies, industry associations, and specified business operators to improve AML/CFT.
- Published the “Issues and practices for dialogue on validation of effectiveness of AML/CFT frameworks,” which sets out concepts and approaches for validationg effectiveness in order to maintain and enhance the frameworks established in accordance with the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism,” in response to evolving ML/TF risks (March 2025)

<Ministry of Agriculture, Forestry and Fisheries and Ministry of Economy, Trade and Industry>

- Conducted inspections on subjects concerning compliance “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Commodity Derivatives Business” (including a risk-based approach) and system development.

<Ministry of Land, Infrastructure, Transport and Tourism>

- Issued requests for reports concerning the actual transaction practices of specified real estate joint ventures and the implementation status of anti-money laundering and combating the financing of terrorism (91 requests in 2024 and 94 requests in 2025) in collaboration with the Financial Services Agency.
- Issued requests for reports to business operators that had not completed establishing frameworks for the matters required under the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism,” in order to ascertain their implementation status (March 2025).
- Held study sessions for prefectural governments and others on anti-money laundering and combating the financing of terrorism (held in August and December 2024).

In addition, following unauthorized access to online securities accounts, in July 2025, the Financial Services Agency and the National Police Agency jointly requested the entire financial industry to strengthen measures against unauthorized access and fraudulent transactions.

(C) Measures by industry associations and business operators

Each industry association supports each financial instrument business operator, etc. and commodity derivatives business operator in implementing AML/CFT by providing a list of cases and examples as well as training.

Financial instruments business operators and commodity derivatives business operators themselves also take measures to establish and strengthen their AML/CFT internal control systems. For example, they set up a division in charge, develop their own rules and manuals, carry out periodic trainings, conduct internal audits, identify transactions that are likely to pose ML/TF risks, and rigorously conduct CDD.

[Examples of Initiatives Taken by Industry Associations]

- In addition to conducting written surveys on the status of member companies' internal control framework, collected information on management systems for AML/CFT, performed risk assessments based on responses from each company, and utilized this information for on-site inspections of the members (Japan Securities Dealers Association, Investment Trusts Association and Japan Investment Advisors Association)
- Formulated and published an audit plan to examine compliance with laws and regulations, including measures such as verification at the time of transaction, preparation and retention of transaction records, and STRs, as well as the status of internal management frameworks for AML/CFT. Based on this plan, conducted audits on members. In addition to issuing audit result notifications to members to facilitate the sharing of understanding regarding AML/CFT, published summaries of the audit results and communicated specific points of attention members (Japan Securities Dealers Association).
- Utilized online platforms to implement training for members (Japan Securities Dealers Association, Type II Financial Instruments Firms Association and the Investment Trusts Association).
- Provided information to members, and conducted awareness-raising activities (Japan Securities Dealers Association, The Financial Futures Association of Japan, Type II Financial Instruments Firms Association, the Investment Trusts Association, Japan Investment Advisors Association and The Commodity Futures Association of Japan).
- Provided an overview of the Act on Prevention of Transfer of Criminal Proceeds and policies on verification at the time of transaction and other information during compliance training offered to members to support AML/CFT implemented by members (The Association for Real Estate Securitization)

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual situation identified by the competent authorities, financial instruments business operators, etc., should continuously pay attention to the following matters for AML/CFT measures:

- When confirming the beneficial owner of a corporate client, implement appropriate measures beyond client declaration by utilizing third-party information sources.
- For foreigner clients, implement appropriate measures, including verifying and retaining the documents used for such verification, as well as requiring the submission of supplementary documents if their residency period has expired.
- Regarding transaction monitoring, enhance the procedure by incorporating additional scenarios for deposit and withdrawal monitoring, and by using IP address tracking to detect cross-border transactions.
- When allowing large-amount cash transactions at the counter, verify and document the reason for having to resort to such transactions at the counter or the source of funds (e.g., whether they are the client's own funds), and assess the presence of suspicious activities.
- Conduct monitoring of cash deposits and withdrawals via ATMs. In cases where frequent ATM deposits or withdrawals of large amounts occur within a short period, investigate whether there is a reasonable explanation for the transactions. If necessary, take appropriate measures such as submitting STRs.

- If issues are identified through guidance from authorities or self-regulatory organizations, establish appropriate corrective measures and ensure sufficient improvements are made by monitoring progress through the internal committees or internal audits.
- Within the group, establish necessary information-sharing and reporting systems, and strengthen collaboration on initiatives.

(v) Assessment of Risks

Financial instruments business operators and commodity derivatives business operators provide products and services for customers to conduct stock investment and commodity derivatives transactions, etc. Offenders planning to engage in ML/TF use such products and services to convert criminal proceeds to various rights, as well as to increase the value of the criminal proceeds.

Some financial instruments business operators manage funds contributed to investment funds. If funds from criminal proceeds are provided for investment funds with complex structures, it becomes difficult to trace the source of funds. Therefore, investments made through financial instruments business operators and commodity derivatives business operators can be an effective method for ML/TF. Indeed, there are cases where criminal proceeds from fraud or embezzlement have been invested in stocks or commodity derivatives. Considering relevant situations, it is recognized that investment made through financial instruments business operators, etc., and commodity derivatives business operators may involve risks of misuse for ML/TF[*1*2].

Furthermore, based on the actual cases where financial instruments business operators or commodity derivatives business operators were misused for ML/TF, in addition to the transactions covered in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes*, transactions under anonymous, fictitious or borrowed names (including suspected ones) are recognized as having an even higher degree of risk.

Competent authorities, financial instruments business operators, and commodity derivatives business operators are taking the above-mentioned risk-mitigating measures taking these risks into account.

However, these efforts differ from one financial instruments business operator to another and from one commodity derivatives business operator to another. Financial instruments business operators and commodity derivatives business operators taking ineffective risk-mitigating measures corresponding to their risks may face a greater risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

[*1] Article 2, paragraph (2), item (xxvii) of the Act on Prevention of Transfer of Criminal Proceeds lists joint real estate enterprises as specified business operators. As of the end of March 2025, the number of entities that have received permission or registration from prefectural governors or competent ministers under the Act on Specified Joint Real Estate Ventures (Act No. 77 of 1994) is 319, and assets acquired using specified joint real estate venture schemes in fiscal year 2023 amounted to approximately 0.4 trillion yen, while assets transferred amounted to approximately 0.2 trillion yen. It is recognized that there is a risk of misuse for the transfer of criminal proceeds in the joint real estate business, which comes from distributing profits arising from the execution of a joint real estate business contract (including a contract for promising the distribution of proceeds from real estate transactions made by delegating the performance of services to one or some of the parties providing funds as a joint business financed by the funds) and which can be used as a way to make it difficult to trace criminal proceeds.

[*2] Article 2, paragraph (2), items (xxxiv) and (xxxv) of the Act on Prevention of Transfer of Criminal Proceeds lists book-entry transfer institutions and account management institutions as specified business operators. It is recognized that the products and services handled by book-entry institutions, which perform services related to book-entry that generate the effect of transferring or pledging bonds and stocks, and account management institutions, which perform services involving account opening for the book-entry transfer of bonds for others (which can be performed by securities companies and banks), may be misused for the transfer of criminal proceeds.

(4) Trust Dealt with by Trust Companies, etc.

(i) Factors that Increase Risks

The trust system is one where a settlor transfers cash, land, or other property to a trustee by the act of trust, and the trustee manages and disposes of the property for a beneficiary pursuant to the trust purpose set by the settlor.

In trusts, assets can be managed and disposed of in various forms. Trustees make the best use of their expertise to manage and preserve assets, and trust is an effective way for companies to raise funds. With these characteristics, trusts are widely used in schemes for managing financial assets, movable property, and real estate as a fundamental part of the Japanese financial system's infrastructure.

Those who intend to operate a trust business as a trust company must obtain registration, a license, or authorization from the competent authorities based on the Trust Business Act (Act No, 154 of 2004). When banks and other financial institutions operate a trust business, they are required to obtain approval from the competent authorities under the Act on Engagement in Trust Business Activities by Financial Institutions (Act No. 43 of 1943). As of the end of March 2025, 99 business operators were engaging in trust business with such a license and authorization[*1].

No cleared ML case involving the misuse of trusts has been reported in Japan in recent years. However, a trust have vulnerabilities for products and services, which are transferability in that a trust does not only mean leaving a property with a trustee but also changing the nominee of a property right and transferring the right to manage and dispose of the property; and complexity in that a trust has a complex scheme to convert pre-trust property into trust beneficiary right, thereby altering the attributes, number and nature of the property rights of the property according to the purpose of the trust.

In its financial sector analysis, the Financial Services Agency has assessed the sector risk of trust as "Low," which means relatively low.

(ii) Trends of STRs

The number of STRs related to trust[*2] between 2022 and 2024 is as follows:

Table 83: The Number of STRs Related to Trust

	2022	2023	2024	Total
Number of STRs Submitted (cases)	37	23	24	84

Among the types listed in *the List of Reference Cases of Suspicious Transactions*, the reason of submitting STRs with the highest number of reports between 2022 and 2024 are as follows:

- Transactions that were conducted before the completion of verification at the time of transaction due to the customer being uncooperative or similar reasons (23 cases, 27.4%).
- Transactions related to Boryokudan gangsters or their related parties (16 reports, 19.0%).

[*1] Refers to the person listed in Article 2, paragraph (2), item (xxv) of the Act on Prevention of Transfer of Criminal Proceeds (trust company), the person listed in item (xxvi) of the same paragraph (company for self-settled trusts), and financial institution engaged in the trust business.

[*2] To calculate the number, STR information was analyzed and relationships with trusts were confirmed.

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transaction, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Trust Business Act and Act on Engagement in Trust Business Activities by Financial Institutions

Stipulates that the Financial Services Agency may requires reports from trust companies and financial institutions engaged in trust activities as necessary if it is deemed that there are issues with their management systems during the conduct of verification at the time of transactions. Moreover, if it is determined that there are significant issues, the Agency may issue an order for business improvement, among other actions.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website’s URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision for Trust Companies	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)

[Examples of Initiatives Taken by Competent Authorities]

<Financial Services Agency>

- Implemented a partial revision of the Notice Regarding the Act on Prevention of Transfer of Criminal Proceeds, adding “transactions as a trustee of a trust” to the examples of types of transactions for savings and deposit agreements (effective June 1, 2023).
- Held meetings to exchange views with industry associations to improve AML/CFT.
- Published the “Issues and practices for dialogue on validation of effectiveness of AML/CFT frameworks,” which sets out concepts and approaches for validationg effectiveness in order to maintain and enhance the frameworks established in accordance with the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism,” in response to evolving ML/TF risks (March 2025).

According to the Financial Services Agency, in transactions of trust companies, the relationship with customers does not only include the initial holders (settlors) and trust companies and equivalent entities (trustees) of the assets such as money or land but also recipients of the transfer of rights to the assets (beneficiaries), forming a tripartite relationship. Furthermore, using a trust makes it possible to separate oneself from these criminal proceeds and conceal one’s connection to these proceeds. Therefore, it is necessary for trust companies, etc., to conduct sufficient verification and risk assessment procedures, not only for settlors but also for beneficiaries as trustees. While some trust companies implement measures commensurate with the risks associated with their beneficiaries, responses vary across trust companies. Consequently, there is a need for trust companies, etc., to conduct risk assessments and CDD based on the characteristics mentioned above.

(C) Measures by industry associations and business operators

Industry associations support the AML/CFT measures taken by each member company by providing training and a range of information from external consulting companies through business communication meetings and study-group meetings on ML. The Association explains to each member company the details to be described in the documents to be prepared by specified business operators according to the intention of each member company, etc., and shares opinions about establishing systems for AML/CFT measures.

Each trust company, etc., is also trying to establish and strengthen its internal control system. For example, when implementing AML/CFT measures, trust companies create documents to be prepared by specified business operators and other documents, prepare rules and manuals, identify transactions that are considered high-risk transactions, and monitor high-risk transactions.

[Examples of Initiatives Taken by Specified Business Operators]

- Implemented identity verification and screening of parties involved in trust schemes after identifying the parties based on the products and services they offer.
- Implemented screening of parties involved, including investment destinations, when managing trust assets based on the associated risks.

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual situation identified by the competent authorities, trust companies, etc., should pay attention to the following matters for AML/CFT measures:

- Establish an appropriate trust agent review and management system, and conduct monitoring and training regularly or as necessary.
- When providing new trust products or services, identify and assess the risks by taking into account specific and individual risks associated with the relevant products or services for identifying and assessing the risks.
- When analyzing the risks, conduct exhaustive and specific analysis, including the analysis of STRs, and ensure the findings are reflected in their AML/CFT risk assessment documents.
- It is necessary to conduct verification at the time of transaction commensurate with the risks, to conduct customer risk assessment considering factors such as products/services, transaction types, countries/regions, and customer attributes, and to establish a continuous CDD system.
- In the sales, management, and audit departments, it is necessary to secure staff with expertise and suitability through recruitment or training.

(v) Assessment of Risks

Trusts have the functions of transferring property rights from a settlor to a trustee, changing the nominee of the property when it is subject to a registration system, and transforming the attribution, quantity, and nature of the property. Furthermore, trusts can only come into force at the conclusion of a trust contract between parties involved or as self-settled trust. Because of such characteristics, offenders attempting ML/TF may be able to separate themselves from criminal proceeds and conceal the relationship with the proceeds if they misuse a trust. No cleared ML/TF case involving misusing trusts has been reported in Japan in recent years. However, these characteristics mean that trusts can be considered as risky for misuse in ML/TF.

Competent authorities and trust companies, etc., are taking the above-mentioned risk-mitigating measures taking these risks into account.

However, these efforts differ from one trust company to another, and trust companies taking ineffective mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(5) Money Lending Dealt with by Money Lenders, etc.

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Lending money or acting as an intermediary for lending money (hereinafter referred to as "money lending," collectively) by money lenders*[1], etc., helps consumers and business operators who need funds to raise money by providing them with convenient financing products and carrying out quick examinations. In addition, with the spread of automatic contract reception machines and automatic teller machines (ATMs), including ones provided by tying up with deposit-taking institutions, and the expansion of transactions through the Internet, money-lending services have become more convenient.

On the other hand, in addition to these conveniences, money lending has characteristics including transferability of rights, which allows those who obtained criminal proceeds make it difficult for the authorities to track their criminal proceeds by misusing money lending, by lending and repaying money repeatedly, and the anonymity of the source of funds in cash transactions. By misusing such vulnerabilities of products and services, money lending can be an effective means of ML/TF.

Those who intend to operate a money-lending business must be registered by a prefectural governor or the Prime Minister in accordance with the Money Lending Business Act (when a business operator seeks to do business with sales branches and business offices in two or more prefectures). As of the end of March 2025, there were 1,473 registered business operators, while the outstanding balance of loans was 41.2240 trillion yen at the end of March 2024.

In its financial sector analysis, the Financial Services Agency has assessed the sector risk of money lending as "Low," which means relatively low.

(B) Typologies

As examples of cases in which the form of criminal proceeds was converted through transactions related to money lending conducted by money lenders and similar entities, the following can be cited:

- Criminal proceeds from robbery and fraud were used to repay money lenders.

There was also an example of money lending related to ML:

- A criminal used a forged image of other person's driver's license to open a bank account in the name of fictitious or other party and applied for a loan contract with a money lender on the Internet to have the money lender transfer the loan into the account.

In addition, although not a loan provided by money lenders, there are the following cases where loan agreements were misused for ML:

- A person operating an investment consulting business had customers enter into a loan agreement with the company regarding the criminal proceeds defrauded under the pretext of investing in an asset management company, and disguised it as a legitimate loan.
- An offender entered into a loan agreement with a partner company and then transferred the money to an account in the company's name as a short-term loan, in order to conceal the criminal proceeds obtained from the illegal export business.

---

*[1] Money Lenders mean those listed in Article 2, paragraph (2), item (xxix) (money lender) and item (xxx) (short-term credit broker) of the Act on Prevention of Transfer of Criminal Proceeds.

(ii) Trends of STRs

The number of STRs submitted by money lenders, etc., from 2022 to 2024 is as follows:

Table 84: The Number of STRs Submitted by Money Lenders, etc.

Category \ Year	2022	2023	2024	Total
Money lenders, etc. (cases)	45,684	63,954	88,282	197,920

The Financial Services Agency revised *the List of Reference Cases of Suspicious Transactions* by adding reference cases focused on abnormal transactions specific to Internet-based transactions and financing of terrorism and released it in March 2022.

The reasons for submitting reports (guideline numbers and names in the “The guideline numbers and names in Guidance for Submitting STRs”) that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 85: Reporting Status of Major STRs by Money Lenders

Reason for report	Number of reports	Percentage (%)
5. Transactions under fictitious or other party’s name	85,134	43.0
43. Customers with unusual behavior or movements	68,637	34.7
42. Transactions related to Boryokudan gangsters or their related parties	12,310	6.2
44. Unusual transactions based on the purpose, occupation or content of business	6,251	3.2
47. Transactions from the same IP address by different customers	3,209	1.6

(iii) Measures to Mitigate Risk

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Money Lending Business Act

Stipulates that the competent authorities may ask money lenders to submit reports, conduct on-site inspections of money lenders, and order money lenders to make business improvements, as necessary.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision for Money Lenders	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)

[Examples of Initiatives Taken by Competent Authorities]
<Financial Services Agency>
- Held meetings to exchange views with industry associations to improve AML/CFT.
- Published the "Issues and practices for dialogue on validation of effectiveness of AML/CFT frameworks," which sets out concepts and approaches for validationg effectiveness in order to maintain and enhance the frameworks established in accordance with the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism," in response to evolving ML/TF risks (March 2025).

(C) Measures by industry associations and business operators

Industry associations have developed self-regulating rules that requires member companies to establish internal control systems by means of making each company's internal rules about the obligation to conduct verification at the time of transactions, submit STRs, and prevent losses caused by Boryokudan gangsters.

Each money lender also takes measures to establish and strengthen its internal control system. For example, when implementing AML/CFT measures, it creates documents to be prepared by specified business operators, prepares rules and manuals, identifies transactions that are considered high-risk transactions, and monitors high-risk transactions.

[Examples of Initiatives Taken by Industry Associations and Specified Business Operators]
<Industry Association>
- Conducted training sessions for lenders aimed at establishing systems required by the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism (Japan Financial Services Association).
- Created and distributed a checklist for establishing an internal system (Japan Financial Services Association)

<Specified Business Operators>
- Enhanced monitoring focused on the similarity of contract contents and suspicious points and implemented initiatives to share points of attention and others through the internal coordination system with relevant departments.

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual situation identified by the competent authorities, money lenders, etc., should pay attention to the following matters for AML/CFT measures:

- When preparing and reviewing their AML/CFT Risk assessment documents, identify and assess the risks exhaustively, not only by quoting the contents of investigation documents or widely used templates, but also by considering the characteristics of the company's transactions, including the products/services, transaction types, countries/regions involved in the transactions, and customer attributes.
- Establish a system for verification at the time of transaction and ongoing CDD commensurate with the risks.

- Regarding IT systems, consider introducing systems or change the settings of existing systems, taking into account the risks they face according to the scale and characteristics of the company's business and transaction types.
- Establish a framework to accurately detect high-risk customers.

(v) Assessment of Risks

Money lending by money lenders, etc., can make tracking criminal proceeds difficult. Considering a relevant situation, it is recognized that money lending by money lenders, etc., carries the risk of misuse for ML/TF. There are cases where an offender carried out loan fraud by identifying himself as a fictitious person and deposited fraudulent money into an account under the fictitious name that had been opened in advance. There is a risk of misuse for generating criminal proceeds.

In addition, based on the cases where money lenders were misused for ML, transactions under anonymous, fictitious, or borrowed names (including those suspected to be such names) are recognized as having an even higher degree of risk besides the transactions covered in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR.

Competent authorities, money lenders, etc., are taking the above-mentioned risk-mitigating measures against these risks.

However, these efforts differ from one money lender to another. Money lenders taking ineffective risk-mitigating measures corresponding to their risks may face a greater risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(6) High-Value Electronically Transferable Prepaid Payment Instruments Dealt with by Issuers

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Prepaid payment instruments are means of payment that users acquire by paying money or other consideration in advance and can use to pay for goods or services up to the value stored. They are issued in various forms, including cards, usage codes, and smartphone applications, and are widely available not only as physical media but also in formats recorded electronically on servers. Electronic money–type prepaid payment instruments and electronic gift certificates fall under this category and are mainly used as small-amount payment methods at specific services or affiliated merchants. In particular, among electronic money-type prepaid payment instruments provided through smartphone applications and similar platforms, some services have tens of millions of users in Japan and are widely used as one of the principal payment methods in the country's cashless society. In 2023, the total issuance amount[*1] of prepaid payment instruments reached 29.9003 trillion yen, and the market size has been expanding year by year.

There are two types of prepaid payment instruments: "self-use type prepaid payment instruments," which can only be used for payments to the issuer, and "third-party type prepaid payment instruments," which can also be used for payments in a broader range of settings such as at affiliated stores. The Payment Services Act mandates that issuers of self-use type prepaid payment instruments with unused balances exceeding a certain amount must notify the Prime Minister, and issuers of third-party type prepaid payment instruments must register with the Prime Minister.

In addition, the Financial Services Agency classifies, for explanatory purposes under the regulatory framework, those third-party-type prepaid payment instruments that can be electronically transferred or assigned as "electronically transferable prepaid payment instruments" among prepaid payment instruments for third party business. Among these instruments, those allowing particularly high-value[*2] deposits and transfers are now positioned as "high-value electronically transferable prepaid payment instruments" under the Act Amending the Payment Services Act and related laws, enacted and promulgated in June 2022. Under the same amendment, issuers of high-value electronically transferable prepaid payment instruments are required to submit a business implementation plan in advance and are designated as specified business operators under the Act on Prevention of Transfer of Criminal Proceeds, thereby being subject to obligations such as verification at the time of transaction, retention of transaction and verification records, and submission of STRs.

In general, under the Payment Services Act, prepaid payment instruments are, in principle, prohibited from being redeemed, and users cannot freely withdraw the amounts they have deposited. This system design, which limits the use of funds to the payment of goods or services, clearly distinguishes prepaid payment instruments from remittance services provided by fund transfer service providers (hereinafter referred to as "fund transfer services").

[*1] See the Japan Payment Service Association website for "Trends in Issuance Amounts of Prepaid Payment Instruments."

[*2] With respect to the monetary thresholds, for stored-balance-type prepaid payment instruments, the amount per transferable instrument's unused balance must exceed 100,000 yen, or the total unused balance transferable within one month must exceed 300,000 yen. For number-notification-type prepaid payment instruments, the amount per unused balance recordable in the prepaid payment instrument account must exceed 100,000 yen, or the total unused balance recordable in that account within one month must exceed 300,000 yen.

Notably, in recent years, there have been cases where prepaid payment instruments and fund transfer functions coexist within a single payment service. While these functions may appear integrated to users, the applicable legal and regulatory requirements differ, resulting in differences in obligations for AML/CFT[*1].

With the development of online platforms and the expansion of services leveraging international credit card payment networks, the usability of prepaid payment instruments has expanded and their functions have become more advanced. Along with the diversification of goods and services that can be purchased and the ease of transferring balances between accounts, some designs also allow third parties to use the instruments through the sharing of usage codes, making their functionality closer to that of cash. In this way, although legal restrictions (such as the prohibition on redemption) remain in place, it has become practically possible to transfer funds and use them anonymously, increasing the risk of being misused for ML/TF. In particular, the combination of transferability, broad usability, and anonymity may amplify inherent vulnerabilities in these products and services, making them potentially effective means for ML/TF.

(B) Typologies

The main cases of misuse of prepaid payment instruments for ML are as follows:

- Using fraudulently obtained credit card information, an offender deposited to an electronic gift certificates (virtual prepaid card) created online under a fictitious name or the name of other party, which was then used for payment of living expenses, and also was used to deposit funds into newly created electronic gift certificates under a fictitious name or the name of other party.
- To receive payment for the sale of illegal videos, the balance of electronic money rights registered under a fictitious identity was increased.
- Products were purchased in stores using electronically obtained electronic money rights of other party, impersonating that other party.
- Using a cash card obtained illegally, an offender operated an ATM to withdraw cash, then used the cash to purchase electronic money rights, and transferred those rights by sending the code number of those rights to another person via social media.
- A business operator that purchases electronic money rights pretended to be a legitimate business when purchasing electronic money rights that had been stolen in online and telephone fraud, and then sold those rights via an online intermediary.
- An offender purchased electronic money rights that had been stolen in online and telephone fraud from another offender who ran an electronic money trading business, and then sold those rights to an electronic money buying business, owned by the offender, pretending to be someone else.

[*1] Even if they function as prepaid payment instruments, issuers of those allowing for withdrawal or remittance of deposited amounts need to be registered as money transfer business operators under the Payment Services Act. Upon such registration, they become specified business operators under the Act on Prevention of Transfer of Criminal Proceeds, thus subject to obligations such as verification at the time of transaction.

(ii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transaction, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Payment Services Act

In June 2022, the Payment Services Act was amended to impose the obligation on issuers of high-value electronically transferable prepaid payment instruments to submit business implementation plans that outline the necessary systems to ensure the prevention of ML/TF, to strengthen monitoring by the administrative authority.

(B) Measures by competent authorities

Efforts such as awareness-raising are being advanced not only from the perspective of preventing ML offences but also from preventing overall crimes by related ministries and industry associations.

- The Ministry of Economy, Trade and Industry, among others, has requested businesses providing cashless payment functions to take adequate measures against unauthorized access (August 2019).
- The Cashless Promotion Council, a general incorporated association, published “Guidelines for Preventing Fraudulent Bank Account Linking in Code Payments” (September 2020) and “Guidelines for Preventing Misuse of Fraudulently Disclosed Credit Card Numbers in Code Payments” (April 2019).

In addition, the competent authorities have also formulated guidelines to ensure that the measures required of specified business operators are properly implemented.

- Published the “Issues and practices for dialogue on validation of effectiveness of AML/CFT frameworks,” which sets out concepts and approaches for validationg effectiveness in order to maintain and enhance the frameworks established in accordance with the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism,” in response to evolving ML/TF risks (March 2025).

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website’s URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Guidelines for Administrative Work (Third volume: Related to finance companies 5 for prepaid payment instruments issuers)	https://www.fsa.go.jp/common/law/guide/kaisya/index.html (Financial Services Agency)

(iii) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, from AML/CFT perspective, issuers of high-value electronically transferable prepaid payment instruments should note that, as they fall within the scope of the Financial Services Agency’s “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism,” it is necessary to establish an internal framework based on these guidelines under the leadership of senior management.

(iv) Assessment of Risks

In Japan, prepaid payment instruments are fundamentally prohibited from being refunded under the Payment Services Act, meaning users cannot freely withdraw cash equivalent to the amount deposited. For many issuers, limits are set on the maximum amount that can be deposited, and the parties to whom the funds can be used are restricted to the issuer or specific affiliated merchants. Accordingly, in terms of system design, certain constraints are imposed on the transferability and convertibility of funds. However, with the advancement of cashless payments, the availability of prepaid payment instruments, including online stores, has expanded, and their forms of use are diverse. Furthermore, because identity verification at the time of transaction is not required for transactions below a certain amount, leaving room for their use as highly anonymous means of transferring funds.

In fact, there have been cases where prepaid payment instruments were misused in the ML process. Particularly in cases of online and telephone fraud, criminals deceive victims into giving away their electronic money rights or electronic gift certificates and then conceal the criminal proceeds by selling the stolen electronic gift certificates through websites that mediate the sale and purchase of electronic money. In light of these circumstances, prepaid payment instruments are recognized as posing a risk of being misused for ML/TF.

Regarding high-value electronically transferable prepaid payment instruments, in particular, although it seems that the number of users actually making high-value deposits and transfers is limited, services allowing deposits of tens of millions of yen are also provided, for example, by international brand high-value electronically transferrable prepaid payment instruments. Moreover, these international brand high-value electronically transferrable prepaid payment instruments, by utilizing the payment infrastructure of the brand’s credit cards, can be used at affiliated stores of the brand, including online, offering the same service functions as the credit cards. Such circumstances further increase the risk associated with high-value electronically transferable prepaid payment instruments.

Furthermore, in light of cases in which prepaid payment instruments have been misused for ML, it is recognized that, in addition to the types of transactions addressed in “Section 4: Risk of Transaction Types, Countries/Regions, and Customer Attributes” of this report, the level of risk becomes even higher where, with respect to the circumstances at the time of the transaction or the attributes of the customer, transactions are conducted anonymously or under fictitious names or borrowed names (including cases where such circumstances are suspected).

In response to such risks, the competent authorities and other relevant bodies have implemented risk-mitigation measures as described above.

However, differences can be observed among business operators with respect to these initiatives. Operators that fail to implement effective risk-mitigation measures commensurate with the level of risk face an increased likelihood of being misused for ML/TF, which in turn may also adversely affect the risk of the industry as a whole.

(7) Funds Transfer Services Dealt with by Funds Transfer Service Providers

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

A funds transfer service refers to the conduct of an exchange transaction service as a business (registration of the appropriate remittance type that corresponds to the amount of each remittance required[*1]) by general business operators other than deposit-taking institutions. With the demand for reasonable and convenient remittance services along with the spread of the Internet, funds transfer services were introduced in 2010 due to deregulation.

Those who intend to operate a funds transfer service must be registered by the Prime Minister under the Payment Services Act. As of the end of March 2025, there were 83 registered business operators. There were 3,522.30 million remittances totaling 10,614.5 billion yen in fiscal 2023. In addition to being used by foreign visitors to Japan as a means of remittance, funds transfer services are increasingly utilized for small-value person-to-person transfers conducted via the internet and other channels, as well as for business-to-business payments. Demand for these services is expected to continue growing in the future (see Table 86).

Table 86: Track Record of Funds Transfer Service Business[*2]

Category \ Year		2021	2022	2023
Number of remittances per year		1,548,782,833	2,341,293,721	3,522,309,038
Break down	Domestic	1,473,790,829	2,263,357,787	3,442,279,199
	Cross-border	74,992,004	77,935,934	80,029,839
Transaction volume per year (million yen)		5,467,864	7,575,681	10,614,548
Break down	Domestic	3,989,725	5,902,381	8,484,095
	Cross-border	1,478,134	1,673,298	2,130,451
Number of registered funds transfer service providers		83	84	83

Note: “Domestic” indicates the number and total value of remittances from within Japan to within Japan, while “Cross-border” indicates the number and total value of remittances from Japan to overseas and from overseas to Japan.

There are three main methods in funds transfer services as follows:

(1) A client requests a funds transfer by bringing cash to the sales office of a funds transfer service provider, and the recipient receives cash at another sales office of the provider;

(2) Funds are transferred between a client’s account and a recipient’s account opened at a funds transfer service provider, or between a sender’s and a recipient’s accounts (or another account of a sender) opened on the website, etc., of the funds transfer service provider; and

(3) A funds transfer service provider issues a card or an instrument (money order) corresponding to money recorded in its server, and payment is made to the person who owns the card or a person who brought in

[*1] For remittances of over 1 million yen permission for Type I Funds Transfer Services, for remittances of 1 million yen or less, permission for Type II Funds Transfer Services, and for remittances of 50,000 yen or less, permission for Type III Funds Transfer Services is necessary.

[*2] See the website of the Japan Payment Service Association (General Incorporated Association), “Trends in Funds Transfer Service Business.”

the instrument.

Among these, in recent years, transfers conducted through accounts (method (2)) have become the mainstream, and providing highly convenient services via smartphone apps and similar platforms has become common. Additionally, there are recent cases in which prepaid payment instruments and funds transfer functions coexist within a single payment service. In such services, actions such as charging, making payments, and transferring funds are all carried out within the same app, making the legal distinctions less apparent. However, because the applicable legal regulations differ, the obligations for AML/CFT also vary.

Furthermore, among providers of funds transfer services, there are operators that do not use the remittance networks of deposit-taking institutions but instead have independently established international funds transfer networks, reflecting a variety of business models. As a result, the risks of misuse for ML/TF vary depending on the services offered by each operator, making AML/CFT challenging and highlighting the difficulty of ensuring transparency in the flow of funds. In particular, in business models involving foreign remittances, differences in legal systems and transaction practices in the countries of use, as well as the difficulty of sharing customer information for verification at the time of transaction, serve as additional risk factors, and the location and level of risk differ among operators. Moreover, in April 2023, a Ministry of Health, Labour and Welfare ordinance came into effect allowing wages to be paid into accounts with funds transfer service providers, further expanding the range of services handled by these operators.

Funds transfer services have characteristics, including transferability, which allows funds to be moved quickly and on a global scale at low fees; extensiveness, which allows funds to be remitted to foreign countries with different legal systems; and anonymity, which allows instructions to be given through non-face-to-face transactions. When these characteristics overlap, tracing the flow of funds becomes particularly difficult. By misusing such vulnerabilities of products and services, funds transfer services can be an effective means of ML/TF.

In light of these circumstances, the Financial Services Agency, in its financial sector analysis, has assessed the sector risk of funds transfer as “High,” which means relatively high.

[Threats and Vulnerabilities Found by Competent Authorities in Recent Years]

- It was discovered that a business operator with global operations established only one set of procedures across countries and did not establish appropriate regulations or procedures for verification of identity and other information at the time of transaction, or screen and monitor transactions in compliance with the laws and regulations of Japan.
- It was discovered that a business operator did not know that its services were contracted out to a subcontractor and sub-subcontractor by its contractor because the business operator did not manage its contractors appropriately.

(B) Typologies

While funds transfer services are increasingly used in diverse forms, such as person-to-person remittances and online payments, due to their low fees and high convenience, cases have also been observed in which they are misused as a means of ML/TF, while outwardly appearing to be legitimate transactions. The following cases are common examples of misusing funds transfer services for ML:

- A dangerous drugs trafficker concealed his proceeds in an account opened in fictitious or other party’s name, and then paid for the procurement of materials to produce drugs from overseas using funds transfer services.

- A foreigner illegally staying in Japan after the expiration of his authorized period of stay, who had visited Japan as a technical intern, used funds transfer services to remit criminal proceeds obtained from selling stolen goods to a foreign crime organization.
- A foreign crime organization carried out a fraud, causing funds to be deposited into bank accounts in Japan, and then remit the money to the foreign crime organization using funds transfer services.
- An offender opened an account for a funds transfer service by impersonating another person with an illegally obtained mobile phone line and bank account information, illegally increased the balance in the account from a linked bank account, and withdrew funds in cash.
- An offender refunded the fraudulent funds that had been transferred to the bank account, then used a multimedia terminal installed in a convenience store to deposit cash into the account of a specified funds transfer service.。

(ii) Trends of STRs

The number of STRs submitted by funds transfer service providers from 2022 to 2024 is as follows:

Table 87: The Number of STRs Submitted by Funds Transfer Service Providers

Category \ Year	2022	2023	2024	Total
Funds transfer service providers (cases)	20,271	29,232	39,122	88,625

The Financial Services Agency revised the List of Reference Cases of Suspicious Transactions by adding reference cases focused on abnormal transactions specific to Internet-based transactions and financing of terrorism and released it in March 2022.

The reasons for submitting reports (guideline numbers and names in the "The guideline numbers and names in Guidance for Submitting STRs") that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 88: Reporting Status of Major STRs by Funds Transfer Service Providers

Reason for report	Number of reports	Percentage (%)
44. Unusual transactions based on the purpose, occupation or content of business	21,396	24.1
16. Economically unreasonable transactions	8,935	10.1
4. Transactions under fictitious or other party's name	7,827	8.8
15. Sudden large deposits, withdrawals and remittances	6,542	7.4
43.Customers with unusual behavior or movements	5,077	5.7

On top of that, funds transfer service providers made some STRs about Money Mules in recent years. In the STRs, typically, a funds transfer services provider asked a customer the purpose of remittance and found out that he had applied for a job offer on a foreign website and had received money and instructions to forward the money to a foreign country.

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transaction, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Payment Services Act

Stipulates that the competent authorities have the right to collect business reports from, conduct on-site inspections, and issue business improvement orders, etc., against funds transfer service providers, as necessary.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Guidelines for Administrative Work (Third volume: for finance companies 14 for funds transfer service providers)	https://www.fsa.go.jp/common/law/guide/kaisya/index.html (Financial Services Agency)

[Examples of Initiatives Taken by Competent Authorities]

<Financial Services Agency>

● Published the "Operational Guidelines (Volume III: Financial Companies – 14. Funds Transfer Service Providers) (Revised January 2025) in response to cases in which operators conduct remittance transactions without obtaining a banking license or registration as a funds transfer service provider, using accounts opened with financial institutions to provide such services. The guidelines, issued in May 2024, stipulate that if information is obtained indicating that an account is being used for foreign exchange transactions by a business suspected of operating without registration, the financial institution that maintains the account may be provided with information regarding the fraudulent use of the deposit account.

● Published the "Issues and practices for dialogue on validation of effectiveness of AML/CFT frameworks," which sets out concepts and approaches for validationg effectiveness in order to maintain and enhance the frameworks established in accordance with the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism," in response to evolving ML/TF risks (March 2025).

● Promulgated the "Partially Amending the Payment Services Act" (Act No. 66 of 2025), applying regulations for funds transfer service providers to cross-border payment receiving agent services (promulgated on June 13, 2025, and scheduled to come into effect within one year).

According to the Financial Services Agency, risks that funds transfer services face are different depending on their transaction amount, business scale, and characteristics. Therefore, the Financial Services Agency requires each funds transfer service provider to establish internal control framework commensurate with the risks corresponding to its transaction amount, business scale, and characteristics appropriately.

However, in identifying and assessing risks, some funds transfer service providers are found to be lagging behind in their efforts of verification at the time of transaction, such as not being able to comprehensively and specifically verify customer attributes due to inaccurate customer information caused by insufficient customer identification at the time of transaction, and not conducting risk assessments based on specific and objective evidence due to not analyzing STRs. Therefore, the Financial Services Agency considers it necessary for funds transfer service providers to comprehensively and specifically identify and assess the risks based on the business scale and characteristics of their business operations. In addition, when a new service is provided using new technology to improve customer convenience, it may not be possible to capture the risk of the service with conventional measures to mitigate. It is necessary for funds transfer service providers to appropriately grasp the risks and take the necessary measures to mitigate risks.

In addition, in September 2025, the Financial Services Agency and the National Police Agency jointly requested financial institutions to strengthen measures, including suspending remittances to the bank accounts of funds transfer service providers resulting from changes in the remitter's name.

(C) Measures by industry associations and business operators

Industry associations support AML/CFT measures taken by funds transfer service providers by developing rules for self-regulation and providing training, among other activities, and have created Q&As or other materials regarding the Act on Prevention of Transfer of Criminal Proceeds, etc. In addition, they have established guidelines to prevent misuse, advising members on the actions they should take to prevent fraud and outlining compensation policies in case of losses, thereby supporting the industry's efforts to prevent misuse.

Funds transfer service providers themselves are endeavoring to establish and reinforce their own AML/CFT internal control systems, too. For example, they have prepared the document prepared by specified business operators, established rules and manuals, screened out transactions that are likely to have higher risks, and adopted enhanced monitoring for transactions with higher risks.

[Examples of Initiatives Taken by Industry Associations]

- Publicized the occurrence and compensation status of losses where malicious third parties open accounts with funds transfer service providers using illegally obtained bank depositor information in that depositors' names, link these accounts with bank accounts, fraudulently deposit funds from the bank accounts to the funds transfer service provider's accounts (fraudulent use of the depositor's bank account spoofing). Also, cases where third parties, having obtained the information of funds transfer service account IDs and passwords illicitly, fraudulently use the account against the users' will without authorization (fraudulent use involving payment account hijacking) were disclosed (Japan Payment Service Association, September 2024).
- Conducted a study session for members in January 2025 and distributed a revised version of the model rules to members in May of the same year to help ensure that member funds transfer service providers have a more robust foundational framework for AML/CFT (Japan Payment Service Association)

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual situation identified by the competent authorities, funds transfer service providers should pay attention to the following matters for AML/CFT measures:

- Establish an appropriate agent review and management system, and conduct monitoring and training regularly or as necessary.

- For customers who open accounts with verification at the time of transaction via bank account transfer procedures, in addition to verifying that there is no impersonation during account opening, conduct a prior screening to ensure compliance with Boryokudan exclusion clauses.

(v) Assessment of Risks

Funds transfer services can be a useful method for ML/TF, given the characteristics of funds transfer services in which foreign exchange transactions are performed as a business, as well as the existence of funds transfer service providers that offer services to remit to many countries abroad and the existence of type I funds transfer services, which allow large amounts of foreign exchange transactions.

In fact, there have been cases where criminal proceeds were transferred abroad through funds transfer services by using third parties who were not involved in predicate offences or by using other person's identification documents and pretending to be the person. There have also been cases where a malicious third party opened an account at a funds transfer service provider under the name of an account holder after obtaining the account information of the account holder illegally, linked the account with a bank account, and illegally deposited funds from the bank account to an account at the funds transfer service provider. Considering these situations, it is recognized that funds transfer services present risks of misuse for ML/TF.

Furthermore, since the deposit-taking institutions are strengthening their AML/CFT countermeasures, there are cases of persons attempting to conduct ML/TF migrating to funds transfer services operated by funds transfer services providers in lieu of goods and services handled by the deposit-taking institutions. This situation is increasing the risk to funds transfer services.

Considering the increase in both the annual number of remittances and the amount handled in the funds transfer business, the expansion of eligibility for funds transfer service providers to participate in the nationwide bank data communication system (Zengin System) in October 2022, and the deregulation in April 2023 allowing wage payments into the accounts of funds transfer service providers (digital wage payments), it can be said that the use of these funds transfer services as a payment method is expanding. Given this situation, we consider the degree of risk that funds transfer services present in terms of misuse for ML/TF to be growing compared to other business categories.

Furthermore, considering the cases where funds transfer service providers were misused for ML, in addition to the transactions described in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, the following transactions are recognized as having an even higher degree of risk:

- Transactions under anonymous or fictitious and borrowed names (including suspected ones)
- Transactions having unusual characteristics or conducted at an unusual frequency considering the purpose of the transactions, occupation, or business of the client, etc.
- Frequent remittance transactions from a large number of persons

In light of such a risk background, the competent authorities and funds transfer service providers are taking the above-mentioned risk-mitigating measures.

However, these efforts differ from one funds transfer service provider to another. Funds transfer service providers taking ineffective risk-mitigating measures corresponding to their risks may face a greater risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(8) Electronic Payment Instruments Dealt with by Electronic Payment Instruments Service Providers

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

In recent years, amidst the digitalization of finance, transactions using so-called stablecoins[*1], which aim to be pegged to the value of legal tender, have rapidly expanded in the United States and other countries. Internationally, discussions regarding user protection and ML/TF issues related to global stablecoins have been held at forums such as the G20 Finance Ministers and Central Bank Governors Meeting, Financial Stability Board (FSB), and the FATF, leading to regulatory considerations in various countries.

In light of these developments, in June 2022, the “Act to Partially Amend the Payment Services Act and Other Related Act” (Act No. 61 of 2022) was promulgated and came into effect on June 1, 2023. These amendments included the introduction of business regulation, such as a registration system for electronic payment instruments service providers[*2], as well as the inclusion of electronic payment instruments service providers as specified businesses under the Act on Prevention of Transfer of Criminal Proceeds, aiming to establish a stable and efficient payment system. To operate as an electronic payment instruments service provider, registration with the Prime Minister is required under the Payment Services Act. As of the end of June 2025, only one entity has been registered as an electronic payment instruments service provider.

Under the Payment Services Act, electronic payment instruments are defined as currency-denominated assets that can be used for payment to unspecified parties and can be bought and sold with unspecified parties, transferable using electronic data processing systems.

Moreover, issuers are limited to fund transfer business operators, trust companies, etc., and intermediaries conducting transactions are defined as electronic payment instruments service providers. In order to operate an electronic payment instrument transaction business, registration with the Prime Minister is required. By establishing these necessary regulations, the framework ensures appropriate user protection and ML/TF measures while also promoting financial innovation utilizing blockchain technology and other initiatives.

The FATF has pointed out the vulnerabilities of so-called stablecoins to ML/TF as follows:

- They have vulnerabilities of being exploited for ML/TF, similar to cryptoassets, due to their high anonymity, the ability to conduct cross-border transactions, and the difficulty of tracking instantaneous transfers.
- The aforementioned vulnerabilities may increase as the service becomes more widely circulated. Since they are more stable in value compared to existing cryptoassets, they may become widely used as a means of payment in society in the future.
- In particular, the use of unhosted wallets for so-called P2P transactions can easily occur, creating a significant vulnerability.
- To mitigate the risks, the issuers and intermediaries should bear obligations for ML/TF measures similar to those of financial institutions and cryptoassets exchange service providers.

[*1] While there is no clear definition of so-called stablecoins, they are generally digital assets that aim for value stability by pegging to specific assets, utilizing distributed ledger technology (or similar technologies).

[*2] Entities listed in Article 2, paragraph (2), items (xxxi-ii) of the Act on Prevention of Transfer of Criminal Proceeds (electronic payment instruments service providers).

- They can become globally available quickly and circulate across multiple jurisdictions, making international cooperation essential to address ML risks adequately.

In this way, electronic payment instruments, like cryptoassets, have characteristics such as anonymity of users in the Internet space, transferability/speed/extensiveness both domestically and internationally, and complexity due to differences in transaction types and regulations between countries. By exploiting such vulnerabilities of products and services, electronic payment instruments can be an effective means for ML/TF.

Although the electronic payment instruments dealt with by electronic payment instruments service providers are currently limited in scope in Japan, they may be used as a means of remittance and payment in a wide range of fields in the future. Additionally, the environment surrounding electronic payment instruments may change rapidly due to their circulation in society and technological advancements.

(B) Typologies

Examples of cases in which electronic payment instruments issued overseas were misused for ML include the following:

- Cryptoassets purchased with cash obtained through fraud were sent to the offender’s own cryptoasset wallet, exchanged for stablecoins, and then transferred to a wallet address controlled by a criminal group.

(ii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, each relevant law and regulation contains on measures to mitigate risks.

○ Act on Prevention of Transfer of Criminal Proceeds

In addition to making verification at the time of transaction mandatory, it stipulates that when electronic payment instruments service providers conclude contracts with an foreign-based electronic payment instruments service providers to transfer electronic payment instruments continuously or repeatedly, they shall confirm that the foreign-based electronic payment instruments service providers have in place a system needed to precisely implement service providers measures equivalent to verification at the time of transaction. It also stipulates that when electronic payment instruments service providers transfer electronic payment instruments, they must inform other electronic payment instruments service providers or foreign-based electronic payment instruments service providers of information regarding the customer and the counterpart of the transfer.

○ Payment Services Act

Stipulates the obligation for electronic payment instruments service providers to submit business reports and, if necessary, allows the competent administrative agency to conduct inspections and issue business improvement orders to electronic payment instruments service providers.

○ FEFTA

Impose the obligation for electronic payment instruments service provider to identify customers and restricted transactions for asset-freezing measures when transferring electronic payment instruments related to customer payments. In addition, it also established compliance standards for foreign exchange transactions service providers and stipulated the obligation to establish internal control framework of asset freezing measures.

(B) Measures by competent authorities

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Guidelines for Administrative Work (Third volume: Related to finance companies 17 for electronic payment instruments service providers)	https://www.fsa.go.jp/common/law/guide/kaisya/index.html (Financial Services Agency)

(iii) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, for the purposes of AML/CFT, electronic payment instruments service providers should pay particular attention to capturing the information of both the sender and the recipient when transferring electronic payment instruments (specified trust beneficiary rights) as defined in Article 2, Paragraph (5), Item (iii) of the Payment Services Act, including through the application of the Travel Rule, in order to mitigate ML/TF.

(iv) Assessment of Risks

Electronic payment instruments, similar to cryptoassets due to their technological similarities, such as using distributed ledger technology, have a high degree of user anonymity and the nature of their transfers being instantaneous and cross-border.

Furthermore, given that they are more stable in value than cryptoassets and that considerations for their use in securities settlement are being advanced in Japan, they may be used as a means of remittance and payment in a wide range of fields in the future. Depending on the changes in the environment surrounding electronic payment instruments due to the future circulation in society and technological advancements, the environment surrounding electronic payment instruments could rapidly change, potentially leading to a swift change in their risk level. Considering these factors, the risk of electronic payment instruments being misused for ML/TF may be relatively higher compared to other business forms.

Additionally, based on cases where cryptoassets transactions have been exploited, aside from the transactions discussed in *Section 4. Risk of Transaction Types, Countries/Regions, and Customer Attributes* in the NRA-FUR, transactions conducted under anonymity or using fictitious names and borrowed names (including those suspected of such) are recognized as having an even higher degree of risk.

In response to such a degree of risk, electronic payment transaction service providers must not only take the measures mandated by law but also proactively implement high-level risk-mitigation measures, including the establishment of ML/TF countermeasure systems equivalent to those of cryptoassets exchange service providers, acquiring and utilizing comprehensive information through continuous CDD and setting flexible monitoring scenarios to detect changes in customer behavior, thus necessitating preemptive measures to mitigate risks.

Moreover, the supervisory authority should guide to maintain that standard and encourage improvements through issuing business improvement orders to business operators that have not implemented appropriate ML/TF countermeasures, indicating the need for continuous measures to reduce risks.

(9) Cryptoassets Dealt with by Cryptoassets Exchange Service Providers

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

In Japan, under the Payment Services Act, cryptoassets such as Bitcoin have proprietary value (limited to that which is recorded on electronic equipment by an electronic method and which excludes Japanese and foreign currencies, assets in currency and electronic payment (excluding those that qualify as currency denominated assets)) that can be used to pay unspecified persons when purchasing goods, etc. and that can be purchased from and sold to unspecified persons as counterparties. They are also defined as currencies that can be transferred using electronic information processing systems. Those who intend to operate cryptoassets exchange service business must be registered by the Prime Minister based on the Payment Services Act. As of the end of June 2025, there are 28 registered business operators. As of the same date, the spot trading volume amounted to 1,395.3 billion yen, and the number of user accounts stood at 12.58 million.

The transaction amounts in cryptoassets are increasing globally, including in Japan, leading to the occurrence of cybercrimes related to cryptoassets. May 2024 saw cases where huge amounts of cryptoassets seemed to be illicitly transmitted from domestic cryptoassets exchange service providers. The background to these cases is considered to be the extremely serious situation that has continued overall in recent years in terms of the threats surrounding cyberspace. For example, the number of cleared cases of cybercrimes in Japan in 2024 was a record high of 13,164 cases, losses caused by ransomware remained at a high level, there were cases of information leaks due to unauthorized access, and cyber attacks by cyber-attack groups supported by states on Japanese cryptoassets exchanges were revealed.

In most cryptoassets have characteristics in which their transfer history is published on the blockchain, so their transactions can be traced. Among the cryptoassets used for transactions by cryptoassets exchange service providers in foreign countries, there are ones that do not disclose transfer records, making it difficult to trace transactions, and that have vulnerability in maintaining and updating their transfer records.

Technologies that increase the anonymity of cryptoassets transactions include:

- “Peel chains,” which involve transferring small amounts of cryptoassets to new addresses consecutively through multiple intermediary addresses.
- “Mixers” and “tumblers,” which use various methods to obscure the connection between the sending and receiving addresses of cryptoassets.
- “Chain hopping,” which involves transfer of cryptoassets multiple times through “bridge,” tools that move assets between non-compatible blockchains, to make tracking more difficult.

The use of these technologies can obscure the trail of cryptoassets transfers, making tracking difficult. In the United States, there have been cases where sanctions have been implemented against companies providing mixing services for assisting in the ML of criminal proceeds.

In addition, in cases where transactions are conducted through cryptoassets exchange service providers located in countries/regions where measures such as identity verification at the time of transaction are not mandatory, transactions conducted by unregistered operators, or where peer-to-peer transactions are conducted using cryptoassets wallets acquired and controlled by individuals, it becomes difficult to identify the owner of the cryptoassets transferred in a transaction. Since almost all transactions handled by cryptoassets exchange service providers are conducted non-face-to-face via the Internet, they have high anonymity and make it easy for offenders to impersonate a third party.

In some foreign countries, there are many cryptoassets ATMs where cryptoassets can be exchanged for legal currency, making cryptoassets more convenient for users. In fact, since there are cases overseas in which drug traffickers convert criminal proceeds derived from drug trafficking into cryptoassets via cryptoassets ATMs using forged identification documents, it is necessary to see how such ATMs are actually being used.

Furthermore, the FATF and other bodies have pointed out risks associated with the linkage between blockchain-based technologies and cryptoassets, citing factors such as the increasing misuse of so-called "stablecoins" for ML/TF purposes, as well as the ongoing occurrence of hacks targeting decentralized finance (DeFi[*1]).

In this way, cryptoassets have characteristics such as anonymity of users in the Internet space, transferability/speed/extensiveness both domestically and internationally, and complexity due to differences in transaction types and regulations between countries. By exploiting the vulnerabilities of products and services, cryptoassets are an effective means for ML/TF.

In its financial sector analysis, the Financial Services Agency has assessed the sector risk of cryptoassets as "High," which means relatively high, considering that there are cases where persons attempting to conduct ML/TF have combined cryptoassets transactions with products and services provided by deposit-taking institutions.

[Threats and Vulnerabilities Found by Competent Authorities in Recent Years]

- There are cases where individuals who have not been registered with the Prime Minister under the Payment Services Act in order to operate cryptoassets exchange service business call for cryptoassets exchanges through social media.
- There are a number of websites that provide guidance to users on how to respond when they receive inquiries from cryptoassets exchange service providers. When analyzing inquiries from cryptoassets exchange service providers to users or responses from users, it is necessary to pay attention to whether the response was based on such guidance.
- It has been observed that cryptoassets exchange service providers, where fraudulent use is on the rise, tend not to implement countermeasures against such misuse adequately. This includes the analysis of methods of fraudulent use and the revision of transaction monitoring scenarios accordingly.
- There was a case where abnormal cryptoassets transactions were not detected because the effectiveness of transaction monitoring scenarios had not been examined, leading to overlooking the implementation of a scenario with specifications that differed from the development requirements.

(B) Typologies

The following cases are common examples of misusing cryptoassets for ML:

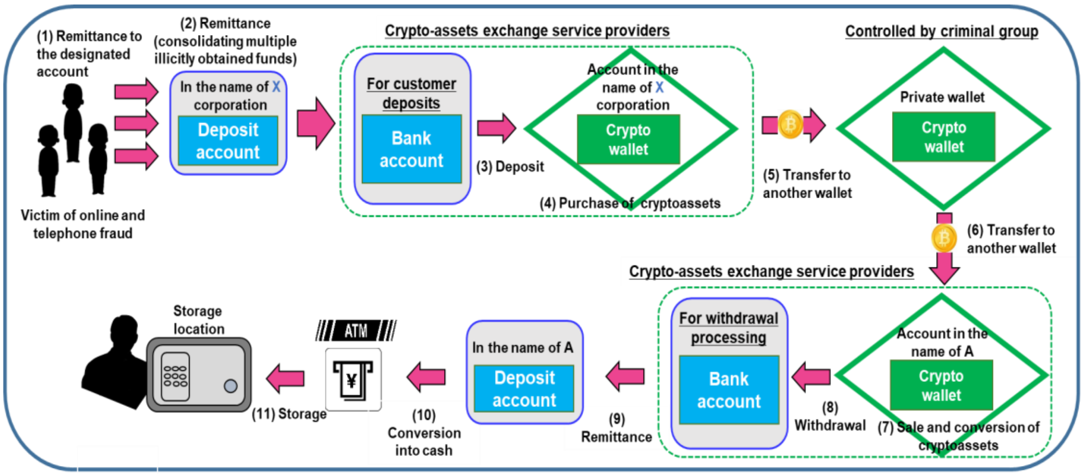
- An offender purchased cryptoassets through an unregistered cryptoassets exchange service provider to disguise the purchase as asset management of funds stolen through FX transaction fraud and received the funds at a cryptoassets wallet managed by the suspect so they could be converted it into cash via a bank

[*1] Decentralized Finance (DeFi). Although there is no clear definition of so-called "DeFi," a February 2022 report by the Financial Stability Board (FSB) describes it as "financial services or products based on distributed ledger technology that are intended to operate without intermediaries.

account.

- An offender transferred cryptoassets obtained through computer fraud to a cryptoassets wallet at a foreign cryptoassets exchange service provider that could be opened in an anonymous name.
- An offender made an employee of a company engaging in transactions for cryptoassets purchase cryptoassets using criminal proceeds that were transferred to an account in the company's name and made the employee convert the cryptoassets into cash via a bank account by transferring the cryptoassets to a crypto wallet managed by the offender and returning almost the same amount of cryptoassets to the crypto wallet of the company account.
- An offender purchased cryptoassets with the criminal proceeds, transferred it through multiple crypto wallets, then sold it for cash, deposited the cash into a bank account in the name of a legal person controlled by the offender, transferred the funds to an account in the offender's name, reimbursed the funds, and delivered the cash to a criminal group.
- An offender transferred criminal proceeds obtained through fraud to a bank account of a cryptoassets exchange service providers under the suspect's control, used automated conversion and remittance programs to exchange the funds into cryptoassets, and then moved the cryptoassets through multiple crypto wallets to a crypto wallet managed by the suspect.

Table 89: Flow of Money Laundering Involving Abuse of Cryptoassets



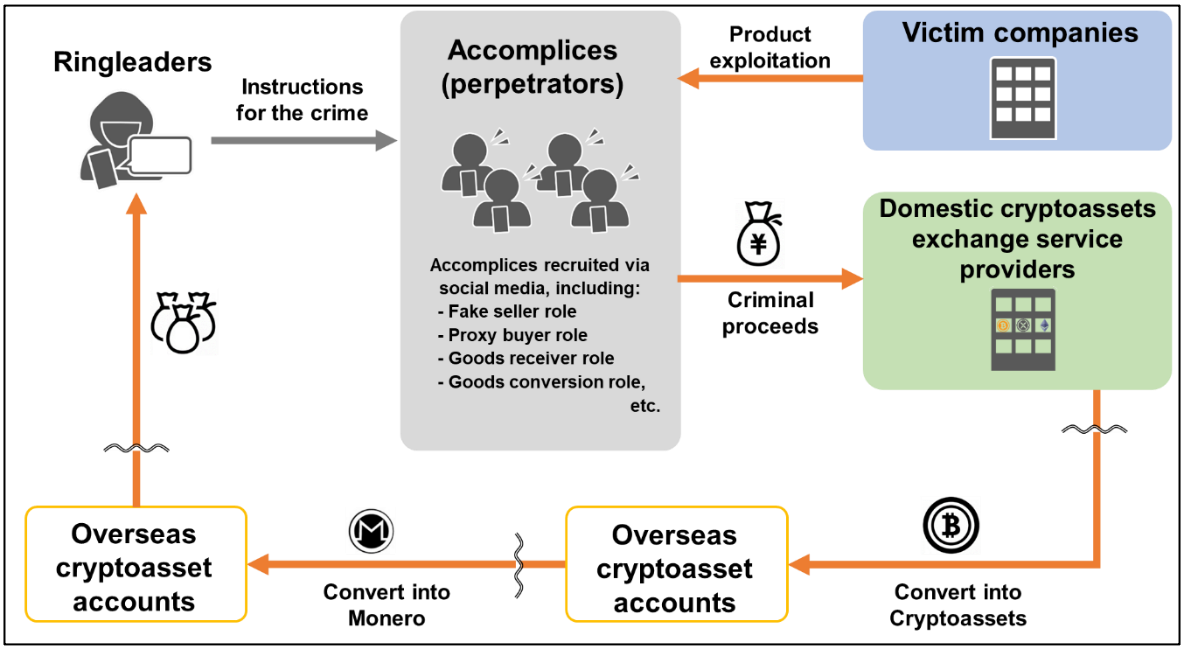
In recent years, violations of the Act on Prevention of Transfer of Criminal Proceeds have been increasing, including cases in which an offender impersonates another person in order to acquire necessary user account IDs and passwords to receive services under a contract for cryptoassets exchange between a customer and a cryptoassets exchange service provider. There have been cases in which the IDs and passwords of cryptoasset accounts opened by foreign students or foreign workers were provided to third parties for a fee.

Furthermore, the following cases are common examples of using cryptoassets as payment in criminal cases:

- A case where cryptoassets were used to pay for illegal drugs purchased on a website in another country.
- A case where ransomware demanded payment in cryptoassets.
- A case where cryptoassets were used by an unlicensed financial instruments business operator to transact financial instruments.

In October 2024, the Joint Investigation Headquarters, including the Cyber Special Investigation Division of the Kanto Regional Police Bureau, apprehended a criminal group that had purchased goods on online flea market services using other people's credit card information, resold the goods, and laundered the proceeds by converting them into Monero, a highly anonymous cryptoasset designed to make transaction history extremely difficult to trace.

Table 90: Overview of Credit Card Fraud Cases



(ii) Trends of STRs

The number of STRs submitted by cryptoassets exchange service providers from 2022 to 2024 is as follows:

Table 91: the Number of STRs Submitted by Cryptoassets Exchange Service Providers

Category \ Year	2022	2023	2024	Total
Cryptoassets exchange service providers (cases)	16,550	19,344	22,667	58,561

The Financial Services Agency created a List of Reference Cases of Suspicious Transactions that includes cases pertaining to transactions on the blockchain and the use of anonymization technologies. It was released in March 2022.

The reasons for submitting reports (guideline numbers and names in the "The guideline numbers and names in Guidance for Submitting STRs") that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 92: Reporting Status of Major STRs by Cryptoassets Exchange Service Providers

Reason for report	Number of reports	Percentage (%)
34. Refusal to provide true beneficiary explanations and materials	8,315	9.4
41. Customers with unusual behavior or movements	6,951	7.8
4. Transactions under fictitious or other party’s name	4,610	5.2
2. Frequent in a short-term, with large total amount of cash	3,133	3.5
35. Transactions in which the true beneficiary is suspicious	2,411	2.7

The details of transactions that are suspected to be made with fictitious or borrowed names are as follows:

- Headshots attached to the principal identification documents of several users with different names and dates of birth were identical
- More than one wallet account opening or user registration was made from the same IP address
- The country of residence of a user was Japan, but the IP address used by the user at the time of login was assigned outside of Japan
- The same mobile phone number was registered as the contact for more than one account and user, but the phone number was not in use

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, each relevant law and regulation contains on measures to mitigate risks.

○ Act on Prevention of Transfer of Criminal Proceeds

In addition to requiring specified business operators to perform identity verification at the time of transactions, the Act stipulates that cryptoassets exchange service providers are required to ensure that foreign-based cryptoassets exchange service providers with which they continuously or repeatedly transfer cryptoassets have in place a system capable of properly conducting measures equivalent to verification at the time of transactions. It also specifies that cryptoassets exchange service providers must inform other cryptoassets exchange service providers or foreign cryptoassets exchange service providers about the customer and the counterparty’s information when transferring cryptoassets.

○ Payment Services Act

Stipulates that the competent authorities have the right to collect reports from, conduct on-site inspection, and issue business improvement orders against cryptoassets exchange service providers as necessary.

○ FEFTA

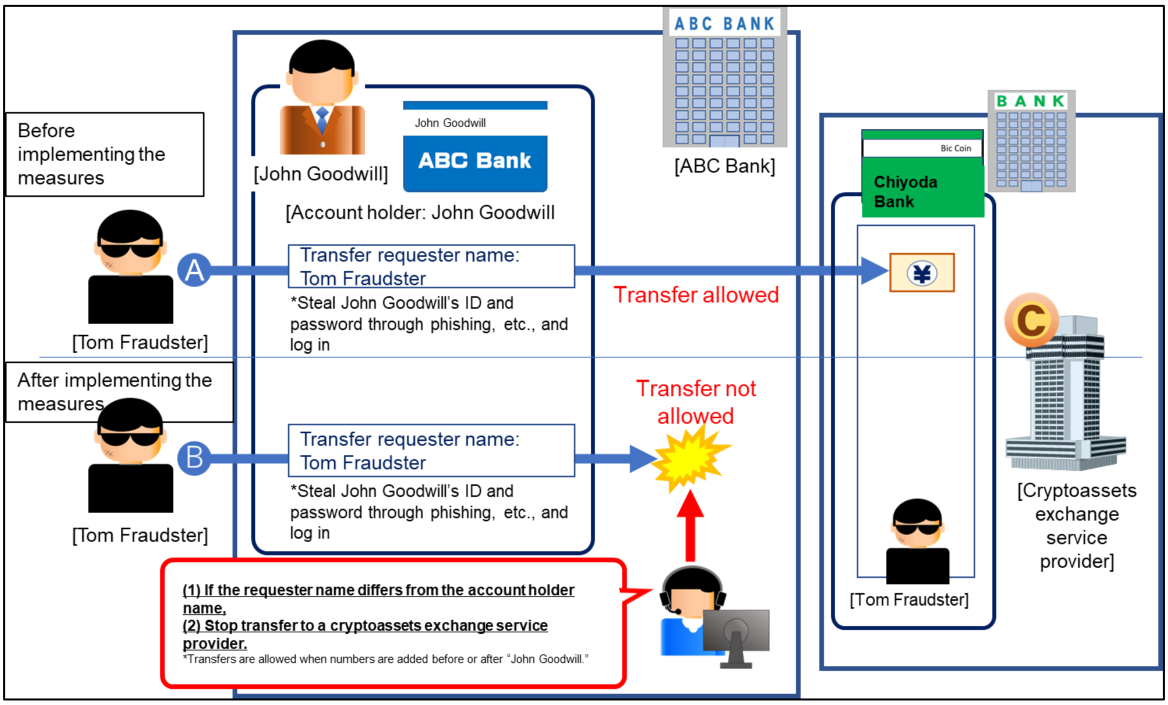
Impose the obligation for cryptoassets exchange service provider to identify customers and restricted transactions for asset freezing measures when transferring cryptoassets related to customer payments. In addition, it also established standards that foreign exchange transactions service providers must comply with and stipulated the obligation to establish internal control framework of asset freezing measures (effective April 1, 2024).

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

Furthermore, in September 2025, the Financial Services Agency and the National Police Agency jointly requested financial institutions to strengthen measures, including suspending remittances to bank accounts of cryptoassets exchange service providers when the remittance name has been altered.

Table 93: Image of Measures Against Fraudulent Transfers to Cryptoassets Exchange Service Providers



[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)
Guidelines for Administrative Work (Third volume: for finance companies 16 for cryptoassets exchange service providers)	https://www.fsa.go.jp/common/law/guide/kaisya/index.html (Financial Services Agency)

[Examples of Initiatives Taken by Competent Authorities]

<Financial Services Agency>

- Raised awareness of users through the Financial Services Agency website and social media to respond to the rise in international fraud cases, etc.
- Issued warnings to unlicensed business operators and took other strict actions against unlicensed business operators in and outside Japan, and raised awareness of users through the website, etc., to respond to reports from users on persons who were suspected to have conducted cryptoassets exchange business without a license.
- Published the "Issues and practices for dialogue on validation of effectiveness of AML/CFT frameworks," which sets out concepts and approaches for validationg effectiveness in order to maintain

and enhance the frameworks established in accordance with the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism," in response to evolving ML/TF risks (March 2025).

(C) Measures by industry associations and business operators

Industry associations have established self-regulatory rules and guidelines based on the Financial Services Agency's "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism," examined the compliance with the laws and regulations as well as self-regulation rules by the members, provided guidance based on the results of the examinations, and raised awareness regarding crimes involving cryptoassets. In addition, in light of *the List of Reference Cases of Suspicious Transactions* for cryptoassets exchange service providers that the Financial Services Agency released in March 2022, the Association is surveying member companies on the status of their STR submissions.

Each cryptoassets exchange service provider has developed and strengthened its internal control system by preparing documents to be prepared by specified business operators, etc., establishing regulations and manuals, identifying high-risk transactions, and strictly monitoring high-risk transitions to implement AML/CFT.

[Examples of Initiatives Taken by Competent Authorities]

<Industry Association>

- Created a document that summarizes key points from "Frequently Asked Questions Regarding 'Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism' (FAQ)" and released it to the members (Japan Virtual and Cryptoassets Exchange Association)
- Conducted follow-ups on the status of member efforts, in order to complete the establishment of internal control framework based on the "Required actions for a financial institution" in the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (Japan Virtual and Cryptoassets Exchange Association)
- Revised self-regulatory rules and guidelines regarding AML/CFT (Japan Virtual and Cryptoassets Exchange Association)

<Specified Business Operators>

- Some cryptoassets exchange service providers have implemented measures to prevent misuse by effectively combining multiple strategies. These strategies include sharing deposit information with banks that provide accounts exclusively for transfer deposits, enhancing their monitoring scenarios, identifying cryptoassets wallet addresses used for illicit withdrawals through blockchain analysis tools, and implementing two-factor authentication during login and deposits/withdrawals.

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, the key matters that cryptoassets exchange service providers should consider for AML/CFT measures are as follows:

- It is necessary to promote the establishment of internal control framework by having the management team take the initiative and actively get involved, give specific instructions, and coordinate with the relevant departments to formulate effective risk mitigation measures and action plans.
- The management department needs to build a system that not only promotes compliance with laws and regulations but also actively practices risk-based approaches and PDCA cycles.
- Internal audits need to go beyond rule-based audits, and audits based on a risk-based approach should be implemented.

- Risk mitigation measures need to go beyond the application of legally mandated requirements such as verification at the time of transaction, and beyond implementing the measures described in the NRA-FUR and widely used templates. The analysis results to be compiled in the AML/CFT risk assessment documents must include the results of a consideration of the sufficiency of risk mitigation measures, particularly from the perspective of a risk-based approach that takes into account vulnerability factors such as non-face-to-face transactions and the high anonymity of cryptoassets themselves. The results must be reflected in the procedures for verification at the time of transaction.
- It is necessary to implement continuous CDD, including management of the period of stay of foreigners, based on the identification and assessment of risks conducted internally.

(v) Assessment of Risks

Cryptoassets allow users to be anonymous and enable instant cross-border transfers. In addition, some countries have no or inadequate regulation on cryptoassets. If cryptoassets exchange service providers in these countries are abused for crimes, it is difficult to trace the transfer of such cryptoassets. Indeed, there have been cases where offenders abused the anonymity of cryptoassets to change them into cash after moving them through foreign cryptoassets exchange service providers and deposit funds in an account under the name of fictitious or other party. For this reason, it is considered that cryptoassets are at risk of misuse for ML/TF.

Additionally, violations of the Act on Prevention of Transfer of Criminal Proceeds, such as providing information necessary for the transfer of cryptoassets to other party, are on the rise in Japan. Furthermore, although deposit-taking institutions have improved their AML/CFT measures, there are cases where persons who intend to commit ML/TF use cryptoassets transactions in addition to products and services handled by deposit-taking institutions. This situation is increasing the degree of risk associated with cryptoassets.

In addition, considering that cryptoassets transactions are increasing globally and the environment surrounding such transactions is rapidly changing, it is recognized that the level of risk for misuse of cryptoassets for ML/TF is relatively high in comparison to other types of business.

Considering these cases, in addition to the transactions covered in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, transactions under anonymous, fictitious and borrowed names (including those suspected to be such names) are recognized as having an even higher degree of risk based on the situation during transactions and customer attributes.

To deal with such a degree of risk, the competent authorities and industry associations have promoted measures to mitigate the degree of risks including the development of a system mentioned above. As a result, remarkable results have been obtained, such as an increase in the number of business operators that obtain and utilize productive information through continuous CDD and that change and detect monitoring scenarios flexibly by keeping track of customer trends. In addition to the risk-mitigation measures described above, the competent authorities and industry associations continue to give guidance for maintaining the level of AML/CFT at business operators. For example, they business operators who have not taken appropriate measures to make improvements by issuing business improvement orders.

Despite the above measures, it is not easy to implement measures to lower the degree of risk immediately in response to the rapid change in the environment surrounding cryptoassets transactions, so cryptoassets exchange service providers need to implement high-level measures in advance. If such measures are not taken sufficiently, cryptoassets exchange service providers will not be able to lower the degree of risk appropriately, and the degree of risk will remain high.

(10) Foreign Currency Exchanges Dealt with by Currency Exchange Operators

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Many Japanese use foreign-currency exchange to obtain foreign currency when they go abroad for sightseeing, business, and the like. Foreign-currency exchange is also utilized by foreign people staying in Japan to get Japanese yen. Currently, foreign-currency exchange operators are roughly divided into deposit-taking institutions and other business operators. The latter group includes hoteliers, travel agencies, and secondhand dealers, in addition to those who specialize in foreign currency exchange. They deal with foreign-currency exchange as a sideline for the convenience of customers in their main business (see Table 94).

Table 94: Transactions by Foreign Currency Exchange Operators

Reporter / Year		2022				2023				2024			
		Number of reporters	Number of transactions	Transaction amount (million yen)	Transaction amount for each transaction (thousand yen)	Number of reporters	Number of transactions	Transaction amount (million yen)	Transaction amount for each transaction (thousand yen)	Number of reporters	Number of transactions	Transaction amount (million yen)	Transaction amount for each transaction (thousand yen)
Deposit-taking institutions	City bank and regional bank	67	74,794	21,158	283	53	157,783	30,334	192	45	101,951	32,293	317
	Shinkin bank	53	1,489	168	113	38	951	109	114	31	872	100	114
	Foreign bank	20	252	369	1,465	20	254	974	3,832	20	306	1,727	5,649
	Other	6	4,294	662	154	6	13,005	1,063	82	6	16,400	816	50
Non-deposit-taking institutions	Funds transfer business/Credit card business	9	74,288	17,432	235	9	160,582	22,219	138	10	217,428	24,208	111
	Hotel business	18	847	147	173	20	6,580	1,352	205	18	5,521	3,423	620
	Travel business	12	431	96	223	13	2,438	186	76	16	3,442	290	84
	Secondhand articles dealer business	42	23,296	3,416	147	58	40,404	4,664	115	80	68,212	7,003	103
	Other	46	81,613	9,699	119	56	212,941	15,873	75	61	356,883	28,872	81
Total		273	261,304	53,147	203	273	594,937	76,773	129	286	771,013	98,731	128

Note: Based on the provisions of Article 18, paragraph (1) of the Ministerial Ordinance on Reporting of Foreign Exchange Transactions, etc. (Ministry of Finance Ordinance No. 29, 1998), the average value of the months reported to the Minister of Finance from January to December of each relevant year was calculated.

In recent years, the number of deposit-taking institutions providing foreign exchange services is decreasing. The number of offices providing foreign exchange services, or the types of currencies handled by deposit-taking institutions providing foreign exchange services, are also decreasing. The number of transactions and the amount of foreign currency exchange temporarily decreased due to factors such as the decline in the number of foreign visitors to Japan and travelers abroad following the spread of COVID-19, but now a recovery is being observed.

Physically taking criminal proceeds overseas lowers the possibility of the existence of such criminal proceeds in Japan being revealed and becoming subject to punishment, confiscation, or other dispositions. Furthermore, if criminal proceeds are converted into foreign currencies and moved across borders, the proceeds can also be used in foreign countries. Foreign-currency exchange have characteristics such as convertibility, which allows the physical form of criminal proceeds to be changed and makes it possible to exchange a large number of small-denomination bills for a smaller number of large-denomination bills, as well as anonymity, which is made possible by non-face-to-face transactions by using foreign currency delivery and automatic foreign currency exchange machines. These characteristics are vulnerabilities as products and services that may be misused for ML/TF.

Japan does not require business operators to acquire any license or registration to operate a foreign-currency exchange business. Anyone can operate the business. In the Third Round of Mutual Evaluation by the FATF, this situation was pointed out as a deficiency. The FATF Recommendation 26 also suggests that businesses providing a currency-exchange service should be licensed or registered, and subject to effective systems for monitoring to ensure compliance with national AML/CFT requirements.

(B) Typologies

The following are common examples of misusing foreign currency exchange for ML:

- Several foreigners visiting Japan converted Japanese yen obtained from thefts in Japan into foreign currencies in multiple transactions by using false names to avoid verification at the time of transactions.
- A drug-trafficking organization used unregistered foreign-currency exchange operators to convert drug proceeds to foreign currency (case in a foreign country).

In addition, although not handled by currency exchange operators, there was the following case where foreign currency exchanges between individuals have been misused for ML:

- An offender transferred the cash obtained through fraud to an account in Japan under the offender’s control, and then transferred foreign currency converted at the exchange rate at the time from an account in a foreign country under the offender’s control to a specified account in a foreign country using foreign currency exchanges between individuals.

(ii) Trends of STRs

The number of STRs submitted by foreign currency exchange operators from 2022 to 2024 is as follows:

Table 95:Trends in the Number of STRs Submitted by Foreign Currency Exchange Operators

Category / Year	2022	2023	2024	Total
Currency Exchange Operators (cases)	430	655	617	1,702

The Ministry of Finance revised *the List of Reference Cases of Suspicious Transactions* for currency exchange operators by adding reference cases focused on abnormal transactions specific to Internet-based transactions and financing of terrorism and released it in October 2019.

The reasons for submitting reports (guideline numbers and names in the “The guideline numbers and names in Guidance for Submitting STRs”) that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 96: Reporting Status of Major STRs by Foreign Currency Exchange Operators

Reason for report	Number of reports	Percentage (%)
1. Large cash transactions	530	31.1
3. Frequent transactions in a short term	360	21.2
15. Customers with unusual behavior or movements	217	12.7
10. Counterfeit or stolen currency	121	7.1
8. Intentional avoidance of identity verification (sudden transaction changes)	88	5.2

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transaction, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ FEFTA

Stipulates that the competent authorities have the right to conduct on-site inspection at and issue business improvement orders against foreign-currency exchange operators as necessary.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website’s URL
Guidelines for Foreign Exchange Transactions Service Providers on Compliance with the Foreign Exchange Act and Its Regulations, etc.	https://www.mof.go.jp/policy/international_policy/gaitame_kawase/inspection/guideline_index.htm (Ministry of Finance)

[Examples of Initiatives Taken by Competent Authorities]

<Ministry of Finance>

- Required for currency exchange operators not only to implement measures to prevent ML under the Act on Prevention of Transfer of Criminal Proceeds, but also to establish frameworks to comply with economic sanctions under the Foreign Exchange and Foreign Trade Act, based on the “Standards for Compliance by Foreign Exchange Transaction Service Providers” established pursuant to the amended Foreign Exchange Act, which came into effect in April 2024. To ensure that these measures are properly implemented by each operator, conducted outreach on concrete methods for complying with these standards, as well as outreach presenting examples of deficiencies detected during foreign exchange inspections.

(C) Measures by industry associations and business operators

Some industry associations that have many members providing foreign-currency exchange services have made voluntary efforts to implement AML/CFT. They have done this by preparing and distributing manuals (templates) for establishing documents to be prepared by specified business operators and internal regulations. Furthermore, they hold regular briefing sessions for members in cooperation with competent authorities and provide support for establishing and reinforcing the internal management of each business operator that exchanges foreign currency.

Foreign-currency exchange operators have prepared documents to be prepared by specified business operators, established regulations and manuals, identified high-risk transactions, strictly monitored high-risk transactions, and made other efforts to establish and improve their internal control systems for implementing AML/CFT.

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, the key matters that currency exchange operators should continue to consider for AML/CFT measures are as follows:

- Appropriately implement verification at the time of transaction based on the provisions of the Act on Prevention of Transfer of Criminal Proceeds, also in cases where the same customer conducts multiple consecutive transactions using a foreign currency exchange machine and the total amount of said transactions exceeds 2 million yen. In addition, since “impersonation transactions,” “suspected fraudulent transactions,” “transactions with customers residing in Iran or North Korea,” and “transactions with foreign PEPs” are transactions for which enhanced CDD is deemed to be particularly necessary, appropriate verification at the time of transaction should be carried out.
- Internal regulations regarding STRs should be formulated taking into consideration the “Reference cases of suspicious transactions involving the sale and purchase of foreign currency or traveler’s checks” published by the Ministry of Finance.
- Provide training to personnel engaged in foreign currency exchange operations so that they can properly fulfill the obligations under the Act on Prevention of Transfer of Criminal Proceeds, such as verification at the time of transaction and submitting STRs.
- When verifying customer identification matters online and non-face-to-face manner, properly record image information provided by customers.
- Refer to reference cases of suspicious transactions and determine whether reporting is required for transactions similar to those cases.
- Properly record the reasons for determining that a transaction is not suspicious.

(v) Assessment of Risks

Foreign currency exchange can be a part of a strategy to take the proceeds of crime abroad. Foreign-currency exchange is usually carried out in cash, offers a high degree of anonymity and can be possessed or transferred without information about the bearer. From these characteristics, foreign-currency exchange can be a useful way to ML/TF.

In fact, there has been a case where foreign currency obtained as criminal proceeds of crime committed abroad was converted to Japanese yen through a third party who did not know the actual circumstances. Considering this relevant situation, it is recognized that foreign-currency exchange carries risks of misuse for ML/TF.

Considering the cases where foreign-currency exchange services were misused for ML, in addition to the transactions described in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, the following transactions are recognized as having an even higher degree of risk based on the situation during transactions, and customer attributes:

- Transactions under anonymous or fictitious and borrowed names (including suspected ones)
- Frequent transactions in a short period
- Transactions in which it is suspected that the customer intentionally avoided verification at the time of transactions
- Transactions related to currency, etc., that was a counterfeit or stolen currency or suspected like that
- Transactions in which it was suspected that the customer was acting on behalf of other people

Competent authorities and foreign-currency exchange operators are taking the above-mentioned risk-mitigating measures in light of these risks.

However, these efforts differ from one foreign currency exchange operator to another. Foreign currency exchange operators taking ineffective risk-mitigating measures corresponding to their risks may face a greater risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(11) Financial Leasing Dealt with by Financial Leasing Operators

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Financial leasing is dealt with by a financial leasing operator, in the form of contracting with a company (lessee) that intends to obtain items such as machinery and vehicles, purchasing the products from a distributor (supplier), and leasing the products to the lessee. Financial leasing has some advantages, for example, a company that intends to obtain equipment can make the payment on an installment plan for a certain period.

Financial leasing has certain characteristics, such as the existence of a supplier in addition to the contracting parties (i.e., a financial leasing operator and a lessee) and a relatively long leasing period. For these reasons, financial leasing may be misused for ML/TF through, for example, a scheme where a lessee and a supplier conspire to engage in fictitious financial leasing. As a vulnerability of products and services, the characteristic of transferability, which makes it easy to transfer funds and goods by disguising the actual state of transactions, can be considered.

(B) Typologies

No cleared ML cases involving misuse of financial leasing have been reported in Japan in recent years. However, there was a case where financial leasing was misused to pay tribute to Boryokudan gangsters. In that case, a person associated with Boryokudan gangsters received goods through financial leasing and allowed a head of the Boryokudan gangsters to use them for a long time.

(ii) Trends of STRs

The number of STRs submitted by financial leasing operators from 2022 to 2024 is as follows:

Table 97: Number of STRs Submitted by Financial Leasing Operators

Category \ Year		2022	2023	2024	Total
Financial leasing operators	(cases)	71	214	141	426

The reasons for submitting reports (guideline numbers and names in the “The guideline numbers and names in Guidance for Submitting STRs”) that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 98: Reporting Status of Major STRs by Financial Leasing Operators

Reason for report	Number of reports	Percentage (%)
16. Transactions related to Boryokudan gangsters or their related parties	251	58.9
9. Multiple lease	36	8.5
8. Empty lease	35	8.2
17. Customers with unusual behavior or movements	21	4.9
3. Transactions under fictitious or borrowed names	15	3.5

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transactions. Also, it stipulates supervisory rights of competent authorities, such as the right to require reports or submission of documents and the right to conduct on-site inspections.

In addition, the Road Transport Vehicle Act (Act No. 185 of 1951) stipulates that no motor vehicles shall be driven if the name and address of the owner, principal place of use, etc., are not registered in the vehicle registration file managed by the Minister of Land, Infrastructure, Transport and Tourism. In effect, most of the leased vehicles are registered ones, so the registration system is useful for mitigate the risks motor vehicle leasing poses.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

[Examples of Initiatives Taken by Competent Authorities]
<Ministry of Economy, Trade and Industry>

- Requested through the Japan Leasing Association to thoroughly inform member companies of "Notification of transactions suspected to be related to Taliban affiliates."
- Conducted outreach to 6 financial leasing operators to confirm the current status of AML/CFT measures in financial leasing operators.
- Conducted risk assessments on financial leasing operators, and formulated guidelines for financial leasing operators by the Ministry of Economy, Trade and Industry, which were thoroughly informed to member companies through the Leasing Association.

(C) Measures by industry associations and business operators

Each industry association supports AML/CFT by each financial leasing operator by preparing and distributing leaflets and pamphlets to announce the establishment of guidelines, providing an overview of the Act on Prevention of Transfer of Criminal Proceeds and matters to be verified at the time of transactions, etc. and providing training.

Respective financial leasing operators also take measures to mitigate risks from transactions that carry a high risk of being misused for ML/TF, establish basic policies and response manuals for AML/CFT measures, provide training for officers and employees, and establish specialized departments to deal with risks, including ML/TF risks.

Furthermore, to prevent transactions that the lessee and the seller collude with each other without actual conditions, in addition to verification at the time of transactions in times of transaction, efforts are made, including the confirmation of the existence of substantial transactions for high-value transactions, and transactions involving new contracts, and leased properties with many accidents.

[Guidelines Established by Industry Associations]

Name of Guidelines	Website’s URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Financial Leasing Business	https://www.meti.go.jp/policy/economy/consumer/consumer/250307leasemanerongl.pdf (Japan Leasing Association)

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, the key matters that financial leasing operators should consider for AML/CFT measures are as follows:

- Establish the necessary frameworks and measures in accordance with the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Financial Leasing Business”
- Refer to “reference cases of suspicious transactions for financial leasing operators” and determine whether STRs should be submitted for transactions similar to those cases.
- Since there have been cases of so-called “empty leases” and “multiple leases” as well as cases where leased items are resold, it is necessary to consider these risks and, if necessary, to physically check the leased items.

(v) Assessment of Risks

Although there were no cleared ML cases involving the misuse of financial leasing, because finance leases have the characteristic of a lessee and a seller being able to conspire to conduct a false transaction, it is considered that finance leases are at risk of being misused for ML/TF.

In light of these situations, etc., in addition to the transactions described in Section *4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, the following transactions are recognized as having an even higher degree of risk based on the situation during transactions and customer attributes:

- Transactions under anonymous or fictitious and borrowed names (including suspected ones)
- Transactions related to financial leasing in which it is suspected of defrauding a financial leasing operator out of money such as multiple financial leasing contracts for the same machinery or equipment

Competent authorities and financial leasing operators are taking the above-mentioned risk-mitigating measures in light of these risks.

However, these efforts differ from one financial leasing operator to another. Financial leasing operators taking ineffective risk-mitigating measures corresponding to their risks may face a greater risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(12) Credit Cards Dealt with by Credit Card Operators

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Credit cards are widely used as a payment method because they are quick and easy to use.

The Installment Sales Act (Act No. 159 of 1961) requires credit card operators to be registered by the Minister of Economy, Trade and Industry if the credit card operators conduct the business of intermediation for comprehensive credit purchases, in which operators provide users with money corresponding to the payment for products over two months or in a revolving form[*1]. As of the end of March 2025, 245 operators were registered.

In recent years, with the spread of e-commerce and cashless payments, the credit card payment market has been continuously expanding. In these circumstances, with the increase in cyber crimes as a background, the losses from fraudulent use of credit cards are expanding, reaching a record high of 55.5 billion yen in 2024.

Credit cards could make it difficult to track criminal proceeds because a holder of criminal proceeds in cash can use a credit card to transform them into different kinds of property.

Furthermore, by user's providing their credit card or credit card information to a third party, it is possible to allow the third party to purchase products. Credit cards can be used all over the world, and some of them have a high maximum usage limit. Therefore, for example, if someone who intends to transfer funds provides a third party with a credit card and makes him purchase a cashable product, and the third party sells the product, it is actually possible to transfer funds in this way, either in Japan or abroad. These characteristics, such as the convertibility of cash into goods and the de facto transferability for use by third parties, are vulnerabilities for products and services. Therefore, credit cards can be an effective means of ML/TF.

> [Threats and Vulnerabilities Found by Competent Authorities in Recent Years]
>
> In some cases of fraudulent use of credit cards, the stolen money is exchanged for cryptoassets and transferred

(B) Typologies

The following cases are common examples of misusing credit cards for ML:

- A store owner engaging in loan-shark business had borrowers make repayments with credit cards by disguising the repayments as payments for meals made by the borrowers, and send false information to credit card companies to receive payments.
- An offender had the criminal proceeds from online and telephone fraud transferred to a bank account linked to the offender's credit card to pay for credit card purchases.
- An offender pretended to put goods up for sale on a shopping site and received payments for drugs by calling them as payments for the goods made with credit cards on the shopping site's payment system.
- An offender had customers at an unlicensed adult entertainment business pay for food and drink using credit card, and had the money deposited in an account in the name of a related party via a credit card payment agency, and then had the money transferred to an account in the offender's name.
- An offender used fraudulently obtained credit card information to increase the balance of electronic money

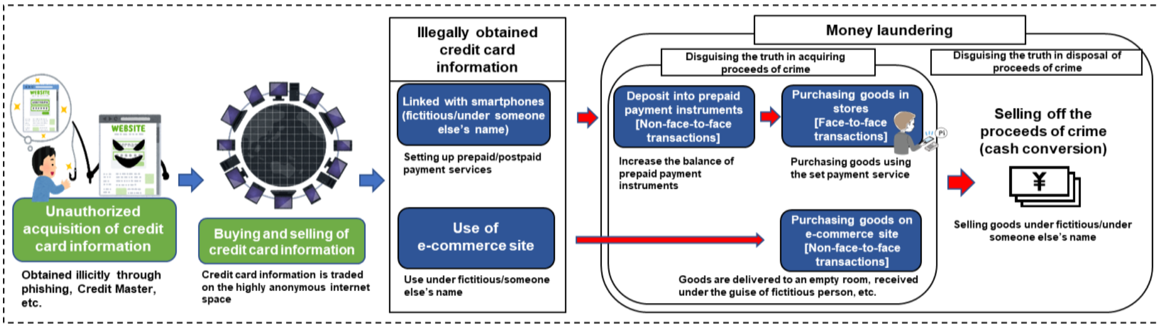
---

[*1] In revolving credit, credit card operators receive an amount of money arrived at by a predetermined method of calculation based on the total cost of products from the user, at regular, predetermined intervals (Article 2, paragraph (3) of the Installment Sales Act).

rights registered under fictitious or other party's names.

- An offender used fraudulently obtained credit card information to set up postpaid payment services on a smartphone registered under a fictitious or other party's name, allowing the impersonation of the cardholder at stores and use of the payment service to purchase goods.
- An offender used fraudulently obtained credit card information to order products online, specifying a fictitious person or an address different from the actual residence as the delivery address, and received the goods.

Table 99: Image of ML Misused by Credit Cards



(ii) Trends of STRs

The number of STRs submitted by credit card operators from 2022 to 2024 is as follows:

Table 100: Trends in the Number of STRs Submitted by Credit Card Operators

Category \ Year	2022	2023	2024	Total
Credit card operators (cases)	41,106	45,674	57,978	144,758

The Ministry of Economy, Trade and Industry revised the List of Reference Cases of Suspicious Transactions for credit card operators by adding reference cases focused on abnormal transactions specific to Internet-based transactions and financing of terrorism and released it in April 2019.

The reasons for submitting reports (guideline numbers and names in the "The guideline numbers and names in Guidance for Submitting STRs") that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 101: Reporting Status of Major STRs by Credit Card Operators

Reason for report	Number of reports	Percentage (%)
3. Transactions under fictitious or other party's name	36,652	25.3
9. Use of cards by those different from the nominees	34,646	23.9
13. Customers with unusual behavior or movements	20,721	14.3
12. Transactions related to Boryokudan gangsters or their related parties	17,114	11.8
1. Issuance of multiple cards over a short period or frequent reissuance	6,075	4.2

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transaction, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Installment Sales Act

- Stipulates that the competent authorities have the right to collect reports from, conduct on-site inspections, and issue business improvement orders against comprehensive credit purchase intermediaries to the extent necessary for the enforcement of the Act.
- Requires a “system necessary for ensuring fair and proper implementation of the intermediation of comprehensive credit purchases” to register as a comprehensive credit purchase intermediary.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

In April 2024, the “Credit Card Security Public-Private Countermeasures Council” was established to share understanding between the public and private sectors on the current situation regarding fraudulent use of credit card, the efforts being made by related business operators, and the direction of countermeasures, as well as to consider the establishment of joint public-private initiatives and systems.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website’s URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Credit Card Companies	https://www.meti.go.jp/policy/economy/consumer/credit/pdf/20211118creditmanerongl.pdf (Ministry of Economy, Trade and Industry)

[Examples of Initiatives Taken by Competent Authorities]
<Ministry of Economy, Trade and Industry>
- Provided specified business operators with training on AML/CFT in collaboration with the industry associations.

(C) Measures by industry associations and business operators

The industry associations have added provisions concerning verification at the time of transactions and STRs to their self-regulatory rules and requested their members to take appropriate measures. Furthermore, the Japan Consumer Credit Association conducted training for members based on the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Credit Card Companies,” which was formulated by the Ministry of Economy, Trade and Industry. The Japan Consumer Credit Association supports measures of each credit card operator by instilling members’ understanding of AML/CFT measures.

By inquiring about credit information institutions designated by the Minister of Economy, Trade and Industry under the Installment Sales Act for information on credit card members, credit card operators can identify any suspicious points, such as a large number of credit card applications made in a short period, and use these findings as references when deciding on the conclusion or renewal of contracts. Additionally, they are setting limits on available amounts through stringent membership and renewal screenings.

Furthermore, voluntary initiatives are being taken to prevent the use of cards by individuals other than the contract holders in face-to-face transactions, including identity verification, screening for transactions considered to be high-risk, intensifying monitoring for transactions with a high degree of risk, implementing systems (such as one-time passwords) to prevent impersonation in non-face-to-face transactions, improving the accuracy of identity verification based on risk through the use of AI and analysis of user behavior, and advancing regular information exchange with regulatory authorities.

[Examples of Initiatives Taken by Industry Associations]

- Provided information, including information on ML, at an information meeting for members in 8 areas in Japan. (Japan Consumer Credit Association).
- Held a 'Briefing session on the responses of credit card companies based on the "Revised Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Credit Card Industry"' to explain the responses requires by credit card operators, and distributed a video recording of the session to the members (Japan Consumer Credit Association).

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, the key matters that credit card operators should consider for AML/CFT measures are as follows:

- When identifying and assessing risks, comprehensively and specifically consider the characteristics of their business and the associated risks, identify the risks they face, and conduct assessment.
- Establish a system for appropriate consideration and judgment on whether a transaction is suspicious, and understand the trends of STRs to enhance their own risk management system.
- Take action in accordance with the "Required actions" and "Expected actions" described in the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Credit Card Business."

(v) Assessment of Risks

Credit cards are recognized as having the risk of misuse for ML/TF because they can transform criminal proceeds into another form of assets by utilizing the credit card and by using fraudulently obtained credit card information to apply for the purchase of goods and then impersonating someone else to receive them, it is possible to disguise the fact of acquiring criminal proceeds.

Considering the cases where credit cards were misused, etc., in addition to the transactions described in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, the following transactions are recognized as having an even higher degree of risk based on the situation during transactions and customer attributes:

- Transactions under anonymous or fictitious and borrowed names (including suspected ones)
- Transactions related to a customer who frequently purchases large amounts of cash equivalent, such as gift cards, by using credit cards

Competent authorities and credit card operators are taking the above-mentioned risk-mitigating measures in light of these risks.

However, these efforts differ from one credit card operator to another. Credit card operators taking ineffective risk-mitigating measures corresponding to their risks may face a greater risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(13) Real Estate Dealt with by Real Estate Brokers

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Real estate has high value and can be converted into a large amount of cash. In addition, real estate valuations may differ significantly depending on the utility value and usage of the property for the parties concerned. These facts make it possible for offenders to transfer criminal proceeds with ease by, for example, paying more than the market value. It is also possible to obscure sources of funds or beneficial owners of real estate by purchasing it under a fictitious or other party's name. These characteristics, such as the anonymity of the source finds and the convertibility between high-value assets and cash, are vulnerabilities for products and services. Therefore, real estate can be an effective means of ML/TF.

Among real estate products, residential lots and buildings are especially valued and actively traded in Japan. Business operators who handle transactions involving these properties are subject to relevant laws and regulations as real estate brokers.

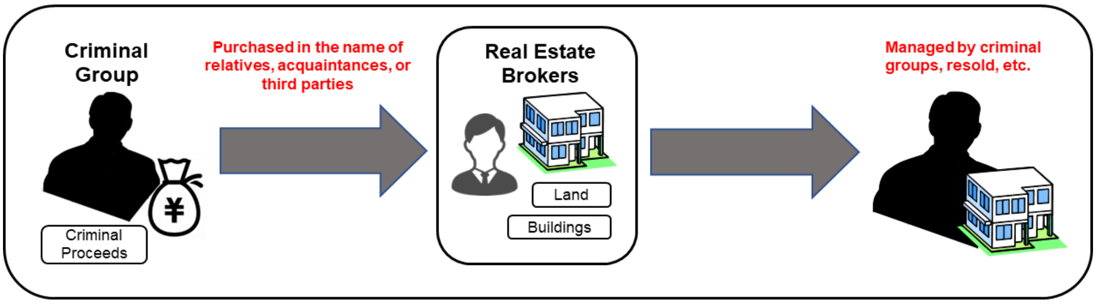
To engage in the real estate brokerage business, it is necessary to obtain a license from a prefectural governor or the Minister of Land, Infrastructure, Transport and Tourism (in cases where the applicant seeks to do business with offices in two or more prefectures) based on Real Estate Brokerage Act (Act no. 176 of 1952). There were approximately 132,291 brokers as of the end of March 2025. In 2023, the annual amount of sales was about 56 trillion yen, and the annual number of effective contracts that were registered with and notified to the real estate information network, which is a designated information network designated by the Minister of Land, Infrastructure, Transport and Tourism in 2024, was about 210,000. Business scale varies significantly across the real estate broker industry. While there are major brokers who handle several thousand transactions a year, there are also small and medium-sized brokers, such as private businesses that operate among their local communities. The latter comprises the majority.

(B) Typologies

The following cases are common examples of misusing real estate for ML:

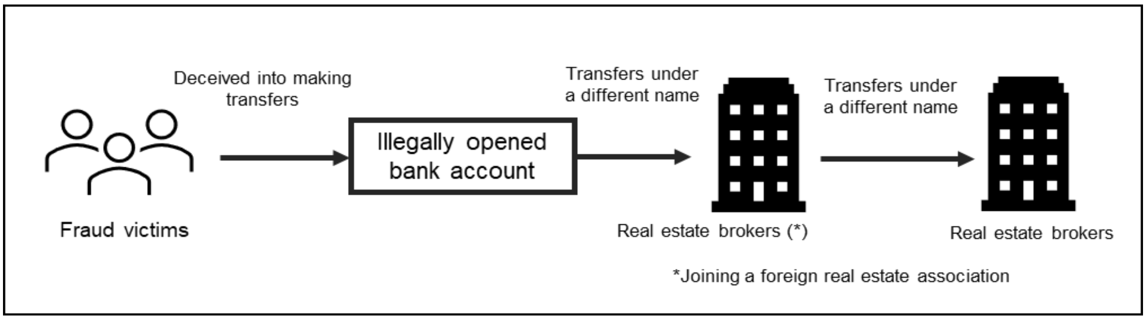
- The proceeds derived from prostitution were used to purchase land in a relative's name.
- A person engaged in real estate brokerage brokered a rental contract in the name of a third party, recorded the brokerage fee as sales from a legitimate rental contract, disguising it as legitimate business revenue.
- A person engaged in money lending and real estate brokerage, when lending money, had people purchase real estate at prices higher than the market price, and then received illegal interest while pretending to receive legitimate real estate purchase proceeds.
- A person engaged in real estate brokerage and rented out a room in a building received cash as rent, knowing that the money was criminal proceeds obtained from selling goods in violation of Copyright Act in the room.
- Drug traffickers purchased real estate for living or for the manufacture of drugs in the name of friends by using proceeds obtained from the illicit sale of drugs (a case in a foreign country)

Table 102: Illustration of ML Using Real Estate Brokers



In addition, an analysis of the flow of funds from online and telephone fraud cases revealed cases in which the proceeds were sent through fraudulently opened bank accounts to real estate brokers and were subsequently suspected of being converted into real estate.

Table 103: A Case in Which The Proceeds of An Online and Telephone Fraud were Transferred to a Real Estate Brokers via a Bank Account



(ii) Trends of STRs

The number of STRs submitted by real estate brokers from 2022 to 2024 is as follows:

Table 104: The Number of STRs Submitted by Real Estate Brokers

Category \ Year	2022	2023	2024	Total
Real estate brokers (cases)	11	18	25	54

The reasons for submitting reports (guideline numbers and names in the “The guideline numbers and names in Guidance for Submitting STRs”) that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 105: Reporting Status of Major STRs by Real Estate Brokers

Reason for report	Number of reports	Percentage (%)
1. Large cash transactions	21	38.9
20. Customers with unusual behavior or movements	5	9.3
2. Large cash amounts over a short period	4	7.4
19. Transactions related to Boryokudan gangsters or their related parties	3	5.6
8. Numerous transactions over a short period	2	3.7

Considering the scale of the industry, it can be said that there are few STRs. However, some of the STRs were submitted from the following perspectives, which are considered to be useful for the entire industry.

- Transactions where a large amount of cash was paid, which was not appropriate for the customers' ages or occupations.
- Suspicious source of funds, such as a customer who tends to stick with cash transactions as their payment method.
- As a result of searching publicly available information regarding the transaction, it was discovered that the customer may have been involved in fraud.
- After investigating the beneficial owners of corporation, they were found to be Boryokudan gangsters.

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transaction, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Real Estate Brokerage Act

- Stipulates that the competent authorities have the right to collect reports from, conduct on-site inspection at, and give guidance to real estate brokers as necessary.
- Stipulates that each real estate broker is required to retain for five years in each of their offices the books containing the names and addresses of the counterparties to each sale and purchase, exchange, or lease contract or of persons who requested the real estate broker to execute such contract on their behalf each time a real estate transaction occurs.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. In order to ensure this, the competent regulatory authorities are taking various measures, including developing and updating supervisory guidelines, formulating the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Real Estate Transactions, thus strengthening risk-based inspection and supervision to assess whether businesses are implementing CDD measures in accordance with these guidelines, and providing lectures and training for industry associations and specified business operators.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Real Estate Transactions	https://www.mlit.go.jp/tochi_fudousan_kensetsugyo/const/tochi_fudousan_kensetsugyo_const_tk3_000001_00040.html (Ministry of Land, Infrastructure, Transport and Tourism)

[Examples of Initiatives Taken by Competent Authorities]

<Ministry of Land, Infrastructure, Transport and Tourism>

- Requested the supervisory authorities to enhance supervision regarding compliance with obligations under the Act on Prevention of Transfer of Criminal Proceeds. This includes focusing on businesses that frequently become subjects of complaints and disputes and those recently licensed by continuing to conduct on-site inspections (Number of business operators inspected in fiscal 2024 was 1,270).

- Issued a notice to industry associations requesting compliance with the Act on Prevention of Transfer of Criminal Proceeds and related laws, as well as strengthened efforts in preparation for the FATF Fifth Round Mutual Evaluation (end of June 2025).
- Held seminars and similar events for industry associations ranging from small to large organizations to raise awareness on the FATF Fifth Round Mutual Evaluation, STRs, and related matters (October 2024 to May 2025).

(C) Measures by industry associations and business operators

The Liaison Council for Preventing Transfer of Criminal Proceeds and Prevention of Damage by Anti-social Forces in Real Estate Business continues to create and distribute materials such as agreements for liaison councils related to the prevention of the transfer of criminal proceeds in the real estate business, as well as booklets for awareness and promotion. Furthermore, the Council continuously follows the status of the FATF's discussion on AML/CFT, exchanges, and shares information among members of the Council, responds to the FATF's mutual evaluation of Japan, and otherwise makes ongoing efforts to operate the system under the Act on Prevention of Transfer of Criminal Proceeds.

The following are recognized as examples of efforts to implement the risk-based approach taken by real estate brokers:

- Information on transactions with customers that were canceled or not performed for some reason in the past is stored in a database for employees in the company to share; and if any subsequent transactions with such customers occur, measures are taken to implement enhanced CDD or to reject those transactions.
- In order not to overlook transactions with Boryokudan gangsters, real estate brokers independently prepare a checklist on the speech and behavioral characteristics of Boryokudan gangsters and utilize the checklist for CDD.

[Examples of Initiatives Taken by Industry Associations]

- Held The "Liaison Council for Preventing Transfer of Criminal Proceeds and Damage Caused by Anti-social Forces in Real Estate Business," composed of industry associations, in September 2024 and January 2025 to raise awareness on strengthening the STRs. In fiscal year 2025, to further enhance efforts, the council is scheduled to meet regularly four times a year in coordination with the National Police Agency and the Ministry of Land, Infrastructure, Transport and Tourism.
- Within the council, created an educational video on fulfilling obligations under the Act on Prevention of Transfer of Criminal Proceeds for member companies and distributed via the council's website (May 2025).

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, the key matters that real estate brokers should consider for AML/CFT measures are as follows:

- When conducting verification at the time of transaction, confirm identification matters using identity verification documents.
- Refer to *the List of Reference Cases of Suspicious Transactions* and consider the necessity for submitting

STRs regarding transactions conducted by the company (including cases where a contract was not concluded).

- Even cases in which a contract is avoided through so-called anti-social force checks, conducted before the conclusion of a sales contract, are subject to reporting. In particular, when inquiries are made using an anti-social force database operated by an industry association and the results indicate a "possible match," STRs should be submitted.

(v) Assessment of Risks

Real estate has high value and can be exchanged for large amounts of cash. Furthermore, it is possible for offenders to transfer criminal proceeds by, for example, paying more than the market value for a property. From these aspects, real estate can be a convenient instrument for ML/TF.

In fact, there have been some cases where criminal proceeds from prostitution or fraud were used to buy real estate. Actually, there have been some cases where criminal proceeds from prostitution or fraud were used to buy real estate. Considering this, real estate presents a risk of misuse for ML/TF. Recently, there have been many cases where real estate was purchased for the purpose of preserving assets or investment, and there is a risk that crime organizations in and outside Japan, etc. have been misusing real estate transactions to change the form of criminal proceeds. For example, conducting a transaction for a large amount that does not match the attributes of the customer requires a response corresponding to the risk, such as verification of the source, etc. of the purchase fund, in addition to the attributes of the customer.

Considering the cases where real estate brokers were misused for ML, in addition to the transactions described in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, it is recognized that transactions under anonymous, fictitious or borrowed names (including those suspected to be such names) are at a higher risk based on the situation during transactions and customer attributes.

Competent authorities and real estate brokers are taking the above-mentioned risk-mitigating measures in light of these risks.

However, these efforts differ from one real estate broker to another. Those not executing CDD measures in accordance with the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Real Estate Transactions or failing to take effective risk-mitigating measures commensurate with their risks may face an increased risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(14) Precious Metals and Stones Dealt with by Dealers in Precious Metals and Stones

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Precious metals and stones have high financial value and are easy to carry because of their small size. They can be easily exchanged with a large amount of cash in any region in the world. In addition, the distribution channel or location of sold and purchased jewelries and precious metals are hard to trace, so they are highly anonymous. As such, the characteristics such as anonymity of the source funds in cash transactions, high financial value, and the easy convertibility into cash are vulnerabilities for products and services. Therefore, precious metals and stones can be an effective means of ML/TF.

The FEFTA requires any person who exports or imports precious metals[*1] of more than 1 kg by carrying them to file a notification to the Minister of Finance in writing, and the Customs Act requires that an export or import declaration of goods mentioned above to the Director-General of Customs must be in writing.

In Japan, offenders have been found to be smuggling precious metals that have high financial value by using the difference between Japan's tax system and that of a foreign country to obtain proceeds illegally. Specifically, offenders can obtain proceeds equal to consumption taxes by purchasing precious metals (gold bullion) in a tax-free country or region, smuggling them into Japan to avoid paying consumption taxes, and selling them at a price that includes consumption taxes.

In the 2023 administrative year[*2], the number of processed cases resulting in sanctions (either referral to prosecutors or notification by the customs commissioner) of gold smuggling was 102 (decrease of approximately 18% compared to the previous administrative year), and the value of evaded taxes was about 360 million yen (approximately 2.1 times compared to the previous administrative year). After the Ministry of Finance developed emergency countermeasures called "Stop Gold Smuggling" in 2017, strengthened the control over gold smuggling, and raised the penal provision against gold smuggling substantially in 2018, the number of cases of gold smuggling resulting in sanctions had been decreasing. However, gold smuggling is on the rise again due to factors such as the rising price of gold and the rapid increase of inbound tourism, so future trends should be closely monitored[*3].

The modus operandi of smuggling has become sophisticated and complex, and gold is being smuggled in small amounts. For example, offenders processed or transformed gold for smuggling in order to conceal it in their body cavities, commercial cargo, or international mail, as well as conducting smuggling through offshore transactions. Meanwhile, smuggling routes have diversified, including the use of airline passengers, air freight, international mail and offshore transactions. When looking in terms of the source of smuggling, Hong Kong, China, Korea, Taiwan and Vietnam account for a large proportion. There is a circulation-type scheme in which offenders purchase gold bullions outside Japan with criminal proceeds obtained from smuggling, smuggle the gold bullions into Japan, and sell them at a store in Japan. Korean smuggling groups and persons affiliated with Boryokudan gangsters and other domestic and international crime groups are involved in such smuggling.

The price of gold fluctuates, and a majority of gold transactions are cash transactions, which is the reason why

---

[*1] Means precious metals set forth in Article 6, paragraph (1), item (x) of the FEFTA.
[*2] The period from July 2023 to June 2024.
[*3] Trends in the number of processed cases of gold smuggling and the value of evaded tax are described in this report under "Chapter 2: Environment Surrounding Japan," "4. Criminal Environment," "(1) Domestic Crime Situation," "(vi) Gold Smuggling."

the transactions are highly anonymous. On the other hand, as a measure to implement AML/CFT, there are some business operators that have stopped accepting cash transactions above a certain amount and have accepted only receiving payments by transfer to an account at a financial institution for such higher-value transactions. In this way, the forms of transactions have changed.

According to the Ministry of Economy, Trade and Industry, when jewelry dealers trade jewelry, payments are usually made with a credit card or by bank transfer, and cash transactions are uncommon. Therefore, from the viewpoint of traceability of funds, the risk of misuse for ML/TF is evaluated as relatively low. On the other hand, there are certain risks for department stores and major jewelers who handle numerous high-priced items. Furthermore, the Ministry evaluates that companies handling precious metals, which often conduct transactions at a scale unsuitable for the company size or transactions with non-residents, have a high risk of misusing them for ML/TF.

(B) Typologies

The following cases are common examples of misusing precious metals and stones for ML:

- An offender forced an acquaintance to sell gold bullion obtained through theft to a gold dealer in the name of a legal person.
- An offender sold stolen ornaments containing precious stones to a pawnbroker by impersonating another person.

These transactions were conducted with an increased level of anonymity, by impersonating to other person or falsifying identification matters, etc., through the presentation of forged IDs at the time of the conclusion of contracts on purchase.

Besides abroad, there was a case where an offender purchased gold bullion using criminal proceeds derived from drug crimes and smuggled them to foreign countries. This shows the actual situation where precious metals and stones are misused for ML due to their high anonymity and ease of liquidation and transportation.

(ii) Trends of STRs

The number of STRs submitted by dealers in precious metals and stones from 2022 to 2024 is as follows:

Table 106: The Number of STRs Submitted by Dealers in Precious Metals and Stones

Category \ Year	2022	2023	2024	Total
Dealers in precious metals and stones (cases)	124	138	223	485

The reasons for submitting reports (guideline numbers and names in the “The guideline numbers and names in Guidance for Submitting STRs”) that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 107: Reporting Status of Major STRs by Dealers in Precious Metals and Stones

Reason for report	Number of reports	Percentage (%)
1. Large cash transactions	128	26.4
17. Frequent in a short-term, multiple transactions	82	16.9
2. Frequent in a short-term, with large total amount of cash	46	9.5
14. Transactions under fictitious or borrowed names	39	8.0
4. Transactions involving multiple individuals and multiple high-value transactions	34	7.0

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transaction, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Secondhand Goods Business Act

Stipulates that police officers have the right to conduct on-site inspections at secondhand goods dealers that handle precious metals and stones, etc., and that the prefectural public safety commissions have the right to order suspension of business of secondhand goods dealers as necessary.

○ Pawnbroker Business Act

Stipulates that police officers have the right to conduct on-site inspections at pawnbrokers and that the prefectural public safety commissions have the right to order the suspension of business of pawnbrokers as necessary.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. In order to ensure this, the competent regulatory authorities are taking various measures, including formulating the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Dealers in precious metals and stones, thus strengthening risk-based inspection and supervision to assess whether businesses are implementing CDD measures in accordance with these guidelines, and providing lectures and training for industry associations and specified business operators.

In order to strengthen risk-based supervision, competent authorities are considering reviewing the questions in the ongoing survey on the implementation status of the Act on Prevention of Transfer of Criminal Proceeds each year, in response to the situation.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines on Anti-Money Laundering and Counter-Terrorist Financing Measures in Precious Metals and Stones	https://www.meti.go.jp/policy/mono_info_service/hoseki_kikinzoku/pdf/guidelines_20220203.pdf (Ministry of Economy, Trade and Industry)

[Examples of Initiatives Taken by Competent Authorities]
<Ministry of Economy, Trade and Industry>

- Thoroughly informed business operators of "Notification of transactions suspected to be related to Taliban affiliates" through industry associations.
- During a training session for member companies hosted by the Japan Bullion Market Association, explained the Guidelines on Anti-Money Laundering and Counter-Terrorist Financing Measures in Dealers in Precious Metals and Stones and discussed compliance issues related to the Act on Prevention of Transfer of Criminal Proceeds. (September 2024)
- Enclosed awareness-raising leaflets prepared by the National Police Agency for the prevention of online and telephone fraud with the questionnaire for the "Survey on the Status of Compliance with the Act on Prevention of Transfer of Criminal Proceeds" sent to dealers in precious metals and stones in order to cooperate with the National Police Agency's measures (October 2024)
- Posted the guidelines prepared by the Ministry of Economy, Trade and Industry on the secondhand dealer–related pages of each prefectural police website to promote awareness of the guidelines among secondhand goods dealers in precious metals and stones in coordination with the National Police Agency (January 2025)
- Prepared a leaflet explaining ML and the obligations under the Act on Prevention of Transfer of Criminal Proceeds, and distributed it at a jewelry exhibition (January 2025).
- Conducted a briefing session on the Act on Prevention of Transfer of Criminal Proceeds for member companies of the Japan Jewellery Association (July 2025).
- Contributed articles explaining the Act on Prevention of Transfer of Criminal Proceeds and the FATF to the newsletter of the Japan Re-Jewelry Council (from July 2025 onward).

(C) Measures by industry associations and business operators

To prevent the purchase of smuggled gold bullion, the Japan Gold Metal Association is acting on gold bullion transactions by requesting operators to check declaration forms and tax payment receipts at Customs for gold bullion brought in from abroad. The Association also endeavors to ensure that its members understand the Act on Prevention of Transfer of Criminal Proceeds by distributing to its members posters, etc., with the nominal support of the Ministry of Economy, Trade and Industry to inform general consumers of the need to present their identification documents for gold bullion transactions; by advertising on its website; and by organizing workshops, with employees of the Ministry of Economy, Trade and Industry and Ministry of Finance as lecturers, for its members that are performing the actual work.

The Japan Jewellery Association makes efforts to ensure that member companies understand AML/CFT measures by preparing and distributing leaflets that describe the overview of the Act on Prevention of Transfer of Criminal Proceeds and the details of their obligations, and updating the website designated for AML/CFT measures.

The Japan Reuse Affairs Association and Antique Dealers Federation of Tokyo are informing their members on AML/CFT by reminding them of the obligations associated with precious-metal transactions under the Act on Prevention of Transfer of Criminal Proceeds in the handbooks for members, and are distributing the handbooks to the members.

The Nationwide Pawnshop Union Alliance Society is raising members' awareness about the Act on Prevention of Transfer of Criminal Proceeds through brochures, its website, and the like for members.

(14) Precious Metals and Stones Dealt with by Dealers in Precious Metals and Stones

Dealers in precious metals and stones are making efforts to establish and strengthen their internal control systems as AML/CFT by regularly getting external audits to acquire international industry certifications, maintaining regulations and manuals, and conducting regular training.

[Examples of Initiatives Taken by Industry Associations]

- Addressed the Act on Prevention of Transfer of Criminal Proceeds in seminars for the Jewelry Remodel Counselor certification examination and included related questions in the examination (ongoing, Japan Re-Jewelry Council).
- Distributed leaflets prepared by the association outlining the Act on Prevention of Transfer of Criminal Proceeds and the obligations required of businesses at jewelry exhibition venues (January and August 2024, and January 2025, Japan Jewellery Association).
- Held a training session for member companies, inviting an official from the Ministry of Economy, Trade and Industry as a lecturer to explain the “Guidelines for Anti-Money Laundering and Counter-Terrorism Financing Measures” and related matters, thereby ensuring thorough awareness of AML/CFT (September 2024, Japan Bullion Market Association).
- Included content on the Act on Prevention of Transfer of Criminal Proceeds in the revised textbook (Sales Volume) for the Grade 3 Jewelry Coordinator certification examination (February 2025, Japan Jewellery Association).
- Published an overview of the Act on Prevention of Transfer of Criminal Proceeds in the “Sustainable Initiatives” guidelines as a related framework for sustainable transactions with customers and business partners (February 2025, Japan Jewellery Association).
- Contributed articles from the Ministry of Economy, Trade and Industry explaining the Act on Prevention of Transfer of Criminal Proceeds and the FATF in the association’s newsletter (from July 2025 onward, Japan Re-Jewelry Council).

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, the key matters that dealers in precious metals and stones should consider for AML/CFT measures are as follows:

- Take action in accordance with the “Required actions” and “Expected actions” described in the “Guidelines on Anti-Money Laundering and Counter-Terrorist Financing Measures in Precious Metals and Stones.”
- Strengthen employee education and training, and establish and review regulations to properly conduct verification at the time of transaction.
- Refer to the List of Reference Cases of Suspicious Transactions and consider the necessity for submitting STRs regarding transactions conducted by the company.

(v) Assessment of Risks

Precious metals and stones have high financial value, are easy to transport and exchanged with cash all over the world, and are highly anonymous because it is difficult to trace their distribution channel and location after transactions. In particular, since gold bullion are usually purchased with cash, they can be an effective method for ML/TF.

Actually, there are cases where offenders pretended to be another person and bought precious metals with cash derived from crimes. Considering this, precious metals and stones present a high risk of misuse for ML/TF.

Considering the cases where dealers in precious metals and stones were misused for ML, in addition to the transactions described in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this

NRA-FUR, it is recognized that the following transactions are at a higher risk based on the situation during transactions and customer attributes:

- Transactions under anonymous or fictitious and borrowed names (including suspected ones)
- The same person/company buying and selling a large amount of precious metals in a short period
- Transactions of frequent purchases resulting in a large amount, even if the purchase amount at the time is small
- Purchases or sales with high value that are not proportionate to the customer's income or assets, etc.

In light of such risks, competent authorities and dealers in precious metals and stones are executing risk-mitigating measures as above mentioned.

However, these efforts differ from one dealer in precious metals and stones to another. Those not executing CDD measures in accordance with the Guidelines on Anti-Money Laundering and Counter-Terrorist Financing Measures in Precious Metals and Stones or failing to take effective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(15) Postal Receiving Services Dealt with by Postal Receiving Service Providers

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

In the postal receiving service business, service providers consent to customers using the service's address or their office address as the place where customers receive mail, to receive the mail for the customer, and to hand it over to customers.

By using a postal receiving service, customers can indicate a place where they do not actually live as their address and receive mail there. Cases exist where postal receiving service providers are misused as a delivery address for money obtained through online and telephone fraud. Such characteristics of creating a fictitious appearance for a business and anonymity through making ownership of transactions unclear are vulnerabilities for products and services. In fact, based on the reports from prefectural police about suspected violations of the obligations to verify identity and other information at the time of transactions and other offences that were revealed during investigations related to online and telephone fraud, etc., the National Public Safety Commission collected 3 reports in accordance with the Act on Prevention of Transfer of Criminal Proceeds from postal receiving service providers between 2022 and 2024. Specific violations identified through the submitted reports are as follows:

- Failed to conduct verification at the time of transaction by documents and verification methods as specified in the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds.
- Neglected to verify the purpose of transactions.
- Failed to retain part of the verification records.
- Failed to record information in the verification records as specified in the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds.

In addition, the Ministry of Economy, Trade and Industry has also assessed that, in particular, business operators who, based on publicly available information, adopt methods for verifying customer identification matters that do not comply with the Act on Prevention of Transfer of Criminal Proceeds and postal receiving service providers who accept non-face-to-face contract applications and who allow customers to use the operators' addresses to register legal persons are at high risk of being misused for ML/TF.

(B) Typologies

The following cases are common examples of misusing postal receiving services for ML:

- An offender received proceeds derived from online and telephone fraud through several locations, including a postal receiving service provider.
- An offender caused repayments to a loan shark and proceeds derived from selling obscene DVDs to be sent to a postal receiving service provider with which a contract was concluded in fictitious or other party's name.

(ii) Trends of STRs

The number of STRs submitted by postal receiving service providers from 2022 to 2024 is as follows:

(15) Postal Receiving Services Dealt with by Postal Receiving Service Providers

Table 108: The Number of STRs Submitted by Postal Receiving Service Providers

Category \ Year	2022	2023	2024	Total
Postal receiving service providers (cases)	1	30	35	66

The Ministry of Economy, Trade and Industry revised and published the List of Reference Cases of Suspicious Transactions, containing newly added reference cases for postal receiving service providers in light of actual states of misuse of postal receiving services. It was released in April 2019.

The reasons for submitting reports (guideline numbers and names in the “The guideline numbers and names in Guidance for Submitting STRs”) that recorded the highest number of reports between 2022 and 2024 are as follows.

Table 109: Reporting Status of Major STRs by Postal Receiving Services

Reason for report	Number of reports	Percentage (%)
2. Refusal to provide true beneficiary explanations and materials	13	19.7
6. Transactions under fictitious or borrowed names	10	15.2

(iii) Measures to Mitigate Risks

(A) Statutory measures

As AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transactions. Also, it stipulates supervisory rights of competent authorities, such as the right to require reports or submission of documents and the right to conduct on-site inspections.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. In order to ensure this, the competent authorities are taking various measures, including formulating and updating the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Postal Receiving Services, thus strengthening risk-based inspection and supervision to assess whether businesses are implementing CDD measures in accordance with these guidelines, and providing lectures and training for specified business operators.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website’s URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Mail Receiving Service Providers	https://www.meti.go.jp/policy/commercial_mail_receiving/pdf/20211224yuubinbutumanerongl.pdf (Ministry of Economy, Trade and Industry)

[Examples of Initiatives Taken by Competent Authorities]
<Ministry of Economy, Trade and Industry>

Conducted 2 cases of reporting collection, 2 cases of on-site inspections, 2 cases of correct order and 3 cases of guidance for postal receiving service providers (during 2024). When a corrective order is issued, the details of the violation and the content of the order are published on the website.

(C) Measures by business operators

The following are recognized as examples of efforts to implement the risk-based approach taken by postal receiving service providers:

- Information on transactions with customers that were canceled or not performed in the past for some reason is shared with other companies in the same industry to strengthen CDD.
- Suspected cases are summarized, and manuals, contract examination standards, contract refusal standards, etc., reflecting such cases in business operations are established.

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, the key matters that postal receiving services should consider for AML/CFT measures are as follows:

- Refer to *the List of Reference Cases of Suspicious Transactions* and consider the necessity for submitting STRs regarding transactions conducted by the company.
- Take action in accordance with the “Required actions” and “Expected actions” described in the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Postal Receiving Services.”

(v) Assessment of Risks

Postal receiving services are misused to provide locations for sending proceeds derived from crime, such as fraud and sales of illegal goods. If falsified customer identification matters are provided to conclude a service contract, it can be difficult to identify the party committing the ML/TF or ownership of the criminal proceeds. Therefore, postal receiving services can be an effective instrument for ML/TF.

In fact, there are cases where offenders made contracts with postal receiving service providers under fictitious names and deceived the providers into receiving criminal proceeds through concealment. Considering this, it is recognized that postal receiving services present a risk of misuse for ML/TF.

Moreover, postal receiving service providers neglect to fulfill their duties under laws and regulations as mentioned above due to deficiencies in their internal control systems, which may increase the risks that postal receiving services present.

Furthermore, considering the cases where postal receiving services were misused for ML, in addition to the transactions described in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, it is recognized that the following transactions are at a higher risk based on the situation during transactions and customer attributes:

- Transactions under anonymous or fictitious and borrowed names (including suspected ones)
- Transactions in which it is suspected that customers might use the service to disguise the company’s actual status
- Transactions with a customer who plans to make contracts for a postal receiving service using multiple companies’ names
- Transactions with customers whose received mails often contains large amounts of cash

In light of such risks, competent authorities and postal receiving service providers need to take the abovementioned measures to mitigate these risks.

However, these efforts differ from one postal receiving service provider to another. Those not executing CDD measures in accordance with the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Postal Receiving Services or failing to take effective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(16) Telephone Receiving Services Dealt with by Telephone Receiving Service Providers

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Telephone receiving service providers consent to use their telephone number as a customer's telephone number, provide services to receive calls to the customer's telephone number, and transmit the content to the customer.

By using such a service, customers can provide telephone numbers that are different from their home or office number, and can receive telephone calls using the provider's number. Because of these characteristics, telephone receiving services are misused in fraud. Such characteristics of creating a fictitious appearance for a business and anonymity through making ownership of transactions unclear are vulnerabilities for products and services.

(B) Typologies

We have not seen a cleared ML case in recent years where a telephone receiving service was misused. However, there have been cases where telephone receiving services were misused to disguise the principal of an ML/TF operation or the ownership of criminal proceeds, such as in a case of fraudulently obtaining public welfare payments.

(ii) Trends of STRs

The number of STRs from telephone receiving service providers between 2022 and 2024 was none.

(iii) Measures to Mitigate Risks

(A) Statutory measures

In order to implement AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transactions. Also it stipulates supervisory rights of competent authorities, such as the right to require reports or submission of documents and the right to conduct on-site inspections.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. In order to ensure this, the competent regulatory authorities are taking various measures, including developing and updating supervisory guidelines, formulating the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Telephone Receiving Services and Telephone Forwarding Services, thus strengthening risk-based inspection and supervision to assess whether businesses are implementing CDD measures in accordance with these guidelines, and disseminating information to specified business operators.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Telephone Receiving Services and Telephone Forwarding Services	https://www.soumu.go.jp/main_content/000810738.pdf (Ministry of Internal Affairs and Communications)

[Examples of Initiatives Taken by Competent Authorities]
<Ministry of Internal Affairs and Communications>

- Posted documents on the website of the Ministry of Internal Affairs and Communications explaining the measures that telephone receiving service providers and telephone forwarding service providers are required to take under the Act on Prevention of Transfer of Criminal Proceeds.
- Conducted a written survey to grasp the status of compliance with laws and regulations as well as risk management by telephone-receiving service providers and telephone-forwarding service providers. (February 2025)
- Issued an overview of the Act on Prevention of Transfer of Criminal Proceeds and information that needs to be verified at the time of transactions to business operators that had provided notification under the Telecommunications Business Act. (July 2025)

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, the matters that telephone receiving service providers should continue to consider for AML/CFT measures are reference to *the List of Reference Cases of Suspicious Transactions* and consider the necessity for submitting STRs regarding transactions conducted by the company.

(v) Assessment of Risks

Recently, we have not seen any cleared cases for ML involving misuse of telephone receiving service providers. However, since telephone receiving services have the characteristic of enabling customers to create a fictitious appearance for their business and to disguise the principal of an ML/TF operation and the ownership of criminal proceeds unclear, it is considered that telephone receiving services present a risk of being misused for ML/TF.

Competent authorities are taking the abovementioned mitigating measures in light of these risks.

However, these efforts differ from one telephone receiving service operator to another. Those not executing CDD measures in accordance with the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Telephone Receiving Services and Telephone Forwarding Services or failing to take effective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(17) Telephone Forwarding Services Dealt with by Telephone Forwarding Service Providers

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

Telephone forwarding service providers consent to the use of their telephone number as a customer's telephone number and provide the service of automatically forwarding calls to or from the customer to the telephone number designated by the customer.

To operate a business as a telephone forwarding service provider, providers must make an application as stipulated in the Telecommunications Business Act (Act No. 86 of 1984). As of the end of March 2025, 1,034 providers had applied to provide telephone forwarding services.

Since customers can receive and make calls by using telephone forwarding services that allow them to show the other party a different telephone number than the actual telephone number of their home, office, or mobile phone and make or receive calls using that alternate number, there have been cases where telephone forwarding services were misused for online and telephone fraud and other crimes. Such characteristics of creating a fictitious appearance for a business and anonymity through making ownership of transactions unclear are vulnerabilities for products and services. These days, there are technologies available that allow telephone forwarding service providers that do not have the facilities or equipment necessary for telephone forwarding services to provide those services, so their customers can show a landline phone number (such as a phone number that starts with 03) through a cloud PBX*[1] owned by other companies. There are cases where a telephone forwarding service provider distributes telephone lines to another telephone forwarding service provider that does not have such facilities or equipment so that the latter can use the cloud PBX owned by the former. Online and telephone fraud cases use the telephone forwarding services of a provider that has purchased telephone lines from another company. This interferes with the investigation of online and telephone fraud cases because it takes time to verify the person who concluded the contract with the telephone forwarding service provider, who is the end client.

In fact, since 2013, a number of reports have been submitted by prefectural police to the National Public Safety Commission stating that telephone forwarding services have been used for crimes such as online and telephone fraud, and that telephone forwarding service providers have been suspected of violating their obligations to verify identity and other information at the time of transactions, etc.

The National Public Safety Commission collected 7 reports from telephone forwarding service providers in accordance with the Act on Prevention of Transfer of Criminal Proceeds during the period from 2022 to 2024. The details of major violations of obligations discovered through these results are as follows:

- Failed to conduct verification at the time of transaction by documents and verification methods as specified in the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds.
- Neglected to verify the purpose of transactions, occupations of customers, etc.
- Failed to record information in the verification records as specified in the rules.

It should be noted that, in some cases, telephone forwarding service providers have avoided regulatory measures intended to correct legal violations by going out of business before a corrective order from the

---

*[1] Services to enable call functions (such as an internal line, an external line, and telephone forwarding) through cloud migration of a private branch exchange (PBX) via a designated line or the Internet.

Ministry of Internal Affairs and Communications and then resuming operations under a new business name.

The Ministry of Internal Affairs and Communications evaluates that, in particular, telephone forwarding service providers that conduct non-face-to-face verifications at the time of transactions, those with few employees that do not have appropriate systems for AML/CFT, and those that purchase telephone lines from other companies are at a high risk of misuse for ML/TF.

(B) Typologies

A case of concealing criminal proceeds derived from the sale of obscene DVDs, multiple telephone-forwarding services contracted under fictitious or other party's name were misused for communication with customers, showing that telephone forwarding services are misused as a means to conceal the owner of the criminal proceeds.

Some telephone forwarding service providers intentionally provide telephone forwarding services, knowing that they are used for crime. There have been cases where such telephone forwarding service providers were arrested for assisting fraud on the grounds that they had facilitated an online and telephone fraud.

(ii) Trends of STRs

The number of STRs submitted by telephone forwarding service providers from 2022 to 2024 is as follows:

Table 110: The Number of STRs Submitted by Telephone Forwarding Service Providers

Category \ Year		2022	2023	2024	Total
Telephone forwarding service providers	(cases)	1	17	5	23

Among STRs submitted by telephone forwarding service providers, there was an STR about transactions under a contract suspected to have been made by impersonation, where the party to the contract told a business operator that they had received a notice by mail about an unfamiliar contract. There was also an STR submitted after a company conducted internal verification of a customer's transactions upon receiving inquiries from public institutions.

(iii) Measures to Mitigate Risks

(A) Statutory measures

In order to implement AML/CFT, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information at the time of transaction, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Telecommunications Business Act

Stipulates that the competent authorities have the right to collect reports from, conduct on-site inspections at, and take other measures against telecommunications business operators to the extent necessary for the enforcement of the Telecommunications Business Act.

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. In order to ensure this, the competent regulatory authorities are taking various measures, including developing and updating supervisory guidelines, formulating the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Telephone Receiving Services and Telephone Forwarding Services, thus strengthening risk-based inspection and supervision to assess whether businesses are implementing CDD measures in accordance with these guidelines, and disseminating information to specified business operators.

Especially given the frequent misuse of telephone forwarding services in crimes such as online and telephone fraud, efforts are being made to prevent the abuse of these services in collaboration with the telecommunications industry groups, namely the Telecommunications Carriers Association (TCA) and the Japan Unified Communications Service provider Association (JUCA). This involves operating a scheme to suspend the use of fixed-line phone numbers and similar measures, thereby restricting the use of fixed-line phone numbers exploited in online and telephone frauds and other crimes. Furthermore, the Ministry of Internal Affairs and Communications is working with the National Police Agency to establish a system that enables the supervision and guidance based on the Act on Prevention of Transfer of Criminal Proceeds and the Telecommunications Business Act, among others, utilizing information on malicious telephone forwarding service providers obtained through the operation of this scheme.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Telephone Receiving Services and Telephone Forwarding Services	https://www.soumu.go.jp/main_content/000810738.pdf (Ministry of Internal Affairs and Communications)

[Examples of Initiatives Taken by Competent Authorities]

<Ministry of Internal Affairs and Communications>

- Revised its scheme to suspend the use of fixed-line phone numbers (inventory numbers) owned by malicious telephone forwarding service providers in bulk when certain conditions are met (June 2023).
- For malicious telephone forwarding service providers, implemented the measure to suspend inventory numbers in bulk for 10,126 numbers from 10 providers in 2024.
- Conducted 2 cases of reporting collection and 1 case of corrective order in accordance with the Act on Prevention of Transfer of Criminal Proceeds (during 2024).
- Conducted a written survey to grasp the status of compliance with laws and regulations as well as risk management by telephone receiving service providers and telephone forwarding service providers. (February 2025).
- Issued an overview of the Act on Prevention of Transfer of Criminal Proceeds and information that needs to be verified at the time of transactions to business operators that had provided notification under the Telecommunications Business Act. (August 2024)
- Provided information on the status of implementation of the Act on Prevention of Transfer of Criminal Proceeds at explanatory meetings hosted by business associations (June 2025).

Commission, the Ministry of Internal Affairs and Communications has conducted reports and specific guidance based on the Act on Prevention of Transfer of Criminal Proceeds to the concerned businesses. In 2024, 1 case of corrective order was issued to telephone forwarding service providers.

The competent authorities are making efforts to improve and correct the issues in which some telephone forwarding service providers are misused for online and telephone fraud, by giving guidance to them.

Suspects of online and telephone fraud misuse the system of telephone forwarding services to show landline telephone numbers on victims' phones when making phone calls from cell phones or to send postcards requesting victims to call telephone numbers disguised as the telephone numbers of government offices. In light of this situation, in September 2019, the National Police Agency and the Ministry of Internal Affairs and Communications launched an initiative requesting major telecommunications providers offering fixed-line phone numbers to take measures such as suspending landline numbers based on the suspension request from the Police if those numbers are used for crimes. In November 2021, specified IP telephone numbers were included in the list of numbers subject to suspension of use.

In addition to these measures, in June 2023, the Ministry of Internal Affairs and Communications revised the scheme to allow for the blanket restriction of all fixed-line phone numbers owned by malicious telephone forwarding service providers, should they meet certain criteria.

(C) Measures by business operators

[Examples of Initiatives Taken by Industry Associations]

- From December 2022, the Japan Unified Communications Service Provider Association, primarily organized by telephone forwarding service providers, newly participated as a subject entity in the scheme for suspending the use of fixed-line phone numbers (Japan Unified Communications Service Provider Association).
- Implementing initiatives to improve measures against the unauthorized use of telephone forwarding services, such as conducting study sessions on laws and regulations, providing courses on verifying identification documents, and developing standard application forms compliant with various laws. Also actively working towards risk reduction by exchanging information with related administrative agencies, providing members with the latest information, and issuing warnings (Japan Unified Communications Service Provider Association).
- Established the Telephone Operator Evaluation Organization (Elite Telecom Operator Certification body, ETOC) by five industry associations related to telecommunications providers, the Telecom Service Association, the Telecommunications Carriers Association, the Japan Internet Providers Association, the Japan Cable Television Association, and the Japan Unified Communications Carriers Association, to operate a new certification system for high-quality service providers (October 2024).

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

In light of the actual conditions identified by the competent authorities, the key matters that telephone forwarding service providers should consider for AML/CFT measures are as follows:

- Verify the purpose of the transaction, the customer's occupation, and other relevant details.
- For corporate customers, identify the beneficial owner.
- Prepare and retain records of the verification.

- In non-face-to-face transactions, send transaction-related documents by registered mail or other methods that do not require forwarding.
- Based on the "Reference Cases of Suspicious Transactions," review the transactions conducted by the company to determine whether STRs are required.
- Take measures to prevent inappropriate use, such as participating in schemes to suspend the use of fixed-line phone numbers.

(v) Assessment of Risks

By using telephone forwarding services, customers can give their business a false appearance and conceal the offenders committing ML/TF or the ownership of criminal proceeds. Thus, it is recognized that telephone forwarding services present a risk of being misused for ML/TF concealing the criminal proceeds obtained from online and telephone fraud, etc.

Moreover, telephone forwarding service providers' neglect to fulfill their duties under laws and regulations as mentioned above due to deficiencies in their internal control systems, which may increase the risks that telephone forwarding services present.

In addition, considering the cases where telephone forwarding services were misused for online and telephone fraud, in addition to the transactions described in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, it is recognized that transactions under anonymous, fictitious and borrowed names (including those suspected to be such names) are at a higher risk.

In light of such risks, competent authorities are taking measures by informing telephone forwarding service providers of their statutory obligations and mitigating the risk through guidance and supervision, including the abovementioned risk-mitigating measures.

However, these efforts differ from one telephone forwarding service provider to another. Those not executing CDD measures in accordance with the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Telephone Receiving Services and Telephone Forwarding Services or failing to take effective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(18) Legal/Accounting Services Dealt with by Legal/Accounting Professionals

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

There are lawyers, etc., judicial scriveners, etc., and certified administrative procedures legal specialists, etc., who possess legal expertise as professionals, as well as certified public accountants, etc., and certified public tax accountants, etc., who possess accounting expertise as professionals.

Lawyers provide legal services at the request of a client or other person concerned. Lawyers must be registered on the role of attorney kept by the Japan Federation of Bar Associations (hereinafter referred to as “JFBA”) and must belong to a bar association that is established in the jurisdiction of each district court. As of the end of March 2025, 46,243 lawyers, 3 Okinawa special members, 525 foreign lawyers, 1,782 legal profession corporations, and 10 foreign legal profession corporations are registered in Japan.

Judicial scriveners provide services related to registration on behalf of clients, consult about registration, and engage in business related to legal representation in summary court. Judicial scriveners must be registered in the judicial scrivener roster kept by the Japan Federation of Shiho-shoshi’s Associations (hereinafter referred to as “JFSA”). As of the end of March 2025, 23,421 judicial scriveners, etc., and 1,286 judicial scrivener corporations are registered.

Certified administrative procedures legal specialists prepare documents to be submitted to public offices and documents relating to rights, duties, or the certification of facts at the request of clients. Other than that, they can carry out procedures as agents to submit documents to public offices. Certified administrative procedures legal specialists must be registered in the administrative scrivener registry kept by the Japan Federation of Certified Administrative Procedures Legal Specialists Associations (hereinafter referred to as “JFCAPLSA”). As of April 2025, 52,734 certified administrative procedures legal specialists and 1,516 certified administrative procedures legal specialist corporations are registered.

Certified public accountants shall make it their practice to audit or attest to financial statements. They may also make it their practice to compile financial statements, to examine or plan financial matters, or to be consulted on financial matters, using the title of certified public accountant. Certified public accountants must be registered on the certified public accountants’ roster or the foreign certified public accountants roster kept at the Japanese Institute of Certified Public Accountants (hereinafter referred to as “JICPA”). As of the end of March 2025, 36,669 certified public accountants, 1 foreign certified public accountants, and 294 audit firms are registered.

Certified public tax accountants represent clients in filing applications and requests, reporting, preparing statements under laws regarding tax payments to tax agencies, preparing tax forms, and consulting about taxation. Other than that, as the incidental business of the mentioned above, they prepare financial forms, keep accounting books on behalf of their clients, and provide a range of services related to finance. Certified public tax accountants must be registered on the roll of certified public tax accountants kept by the Japan Federation of Certified Public Tax Accountants’ Associations (hereinafter referred to as “JFCPTAA”). As of the end of March 2025, there were 81,696 certified public tax accountants and 5,146 certified public tax accountants’ corporations registered.

As mentioned above, legal/accounting professionals possess expertise in law and accounting. They have good social credibility and are involved in a wide range of transactions.

However, for those who attempt ML/TF, legal/accounting professionals are useful because they have indispensable expertise in legal/accounting fields to manage or dispose of property for those purposes. At the same time, due to their high social credibility, involving these professionals in transactions or asset management can create the appearance of legitimacy, making them particularly useful from the perspective of those seeking to conceal illicit activities.

Furthermore, the FATF etc. points out that since restrictions are effectively imposed on banks, etc., persons who plan to engage in ML/TF are using other methods for ML/TF, such as obtaining advice from legal or accounting professionals and by involving legal or accounting professionals who have social credibility in their transactions instead of using banks.

These characteristics, such as the anonymity and the complexity of transactions, using the highly specialized knowledge and social credibility of legal/accounting professionals to create the appearance of legitimacy, are vulnerabilities for products and services, which may be misused for ML/TF.

(B) Typologies

The following cases are common examples of misusing legal/accounting services for ML:

- A loan shark asked a judicial scrivener to provide services for incorporation on its behalf, set up a shell company, deceived deposit-taking institutions to open accounts for the cooperation, and misused the accounts to conceal criminal proceeds.
- An innocent certified public tax accountant was used for the bookkeeping of proceeds derived from fraud in order to disguise them as legitimate business profits.
- An offender asked a judicial scrivener, who was unaware of the situation, to set up a corporation using criminal proceeds obtained from fraud, etc., and opened a bank account in the company’s name to deposit criminal proceeds into the bank account.
- A former Boryokudan gangster used part of the cash obtained through fraud, which constituted criminal proceeds, and enlisted a judicial scrivener who was unaware of the circumstances to establish a company with a relative as the representative director, for the purpose of controlling the management of the corporation’s business.

Also, the following case is an example abroad.

- A case where an illicit dealer of drugs disguised proceeds derived from drug crime as compensation paid by the purchaser of a building who was an accomplice. A lawyer who knew nothing about the circumstances was used as the agent for the sale/purchase of the building.

Thus, actual situations do exist where persons attempting to launder money use legal- and accounting-related services to disguise acts of concealing criminal proceeds as legitimate transactions.

(ii) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds imposes the obligation to conduct verification at the time of transaction (for certified administrative procedures legal specialists, etc., certified public accountants, etc., certified public tax accountants, etc., this includes verification of assets and income status in the case of high-risk transactions) and the obligation to prepare and preserve verification records and records of agent work, etc. for specified mandated acts on legal and accounting professionals (excluding lawyers, etc.) for certain transactions.

The Act also sets forth the supervisory measures by competent authorities, such as requiring reports or the submission of documents and on-site inspections.

It also stipulates that certified administrative procedures legal specialists, etc., certified public accountants, etc., and certified public tax accountants, etc., are required to submit STRs except for matters pertaining to the confidentiality obligations. As for judicial scriveners, etc., the JFSA and each judicial scriveners' association provide alternative measures to STRs in the associations' rules.

As for lawyers, etc., the JFBA sets rules and regulations that stipulate the duties of lawyers pursuant to the provisions of the Act on Prevention of Transfer of Criminal Proceeds. These include the verification of Client Identification Matters, etc. with regard to certain transactions, the preparation and retention of verification records and transaction records, and avoiding the provision of services if there is any suspicion of misuse for ML/TF. In addition, the JFBA has established measures equivalent to verification at the time of transaction, by requiring individual lawyers to submit an annual report regarding verification of Client Identification Matters, etc. and retention of records and other matters.

Table 111: Obligations of Legal/Accounting Professionals under the Act on Prevention of Transfer of Criminal Proceeds

<table>
<tr><th>Category</th><th>Verification of customer identification matters</th><th>Confirmation of transaction purposes etc.</th><th>STR</th></tr>
<tr><td>Lawyers, etc.</td><td>Association's Rules (Article 12)</td><td>Association's Rules (Article 12)</td><td rowspan="2"></td></tr>
<tr><td>Judicial scriveners, etc.</td><td rowspan="4">The Act on Prevention of Transfer of Criminal Proceeds (Article 4)</td><td rowspan="4">The Act on Prevention of Transfer of Criminal Proceeds (Article 4) (Note 1)</td></tr>
<tr><td>Certified administrative procedures legal specialists, etc.</td><td rowspan="3">The Act on Prevention of Transfer of Criminal Proceeds (Article 8) (Note 2)</td></tr>
<tr><td>Certified public accountants, etc.</td></tr>
<tr><td>Certified public tax accountants, etc.</td></tr>
</table>

Note 1: For judicial scriveners, etc., the obligation to confirm assets and income status is excluded.
2: Matters subject to confidentiality obligation are excluded.

(B) Measures by competent authorities and self-regulated organizations

Each competent authority and each association of legal and accounting profession are also making efforts to promote AML/CFT measures, such as by developing regulations, preparing materials about duties, and providing training, thus promoting an understanding of ML/TF risks to legal and accounting professionals.

(a) Japan Federation of Bar Associations (JFBA) and Regional Bar Associations

In light of the enforcement of the amended Act on Prevention of Transfer of Criminal Proceeds on April 1, 2024, the JFBA revised the regulations related to AML/CFT for lawyers and others, as well as the format of the annual reports submitted by lawyers to their bar associations. Accordingly, the JFBA informed its members of these revisions in preparation for the implementation of the revised formats in April 2025. Furthermore, in order to encourage lawyers, etc., to understand the ML risks associated with their legal practice, the JFBA has conducted interviews and follow-up investigations on the responses to annual reports for law firms, analyzed high-risk categories of businesses, compiled the results into the Legal Practice Risk Assessment for ML, which was published in the JFBA's journal that is distributed to all members. In addition, the JFBA prepared tools, FAQs, and online courses to promote compliance with the regulations concerning AML/CFT by lawyers, etc., and provided them to lawyers, etc., and bar associations. The JFBA also supports each lawyer in enhancing AML/CFT by posting information on efforts made by law firms as well as ML risks that arise in connection with new technologies on its website to inform its members of AML/CFT and share information.

In light of the actual situation identified by the JFBA, lawyers, etc., should pay attention to the following matters for AML/CFT measures:

- Refer to the Legal Practice Risk Assessment for ML and analyze and evaluate risks in their service.
- Refer to the results of the above risk analysis and assessment, and carefully consider whether the purpose of the request is related to the transfer of criminal proceeds in light of the attributes of the client, the business relationship with the client, the content of the request, and respond appropriately.

Moreover, each bar association takes remedial actions as needed to lawyers, etc., who are considered to face risks based on their submission status and the contents of the annual report.

Through risk-based monitoring, the JFBA states that improvements can be seen in the status of the members' submission of annual reports and the status of their fulfillment of obligations regarding AML/CFT measures.

(b) Ministry of Justice and JFSA

JFSA promotes judicial scriveners, etc., to understand the risks associated with their services by holding training sessions and publishing articles on AML/CFT measures on its journal, Monthly Report Judicial Scrivener.

Additionally, the JFSA is considering the creation of guidelines related to AML/CFT measures. It is also engaging in efforts to disseminate information regarding the impact on judicial scriveners' work, such as organizing explanatory sessions and meetings for judicial scriveners' association representatives within block associations, as well as creating and raising awareness of video content for its members.

Furthermore, pursuant to the enforcement of the amended Act on Prevention of Transfer of Criminal Proceeds (April 1, 2024), the Ministry of Justice, in collaboration with the JFSA, formulated and published the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Work of Judicial Scriveners and Judicial Scrivener Corporations" on April 1, 2024, which aim to outline a framework for a risk-based approach for judicial scriveners, etc., and ensure their compliance with the framework. The JFSA has created and distributed a "Guideline for the Risk-Based Approach (Concepts)," as well as prepared the "Collection of Reference Cases of Risk Factors for Money Laundering and Terrorist Financing for Shiho-Shoshi Lawyers," and training DVDs.

In light of the actual situation identified by the competent authorities, matters that judicial scriveners, etc. should pay attention to for AML/CFT measures are appropriate verification at the time of transaction by receiving the submission of identity verification documents. The competent authorities are trying to improve and correct these by giving guidance to judicial scriveners, etc. Besides, the competent authorities evaluate that there is a risk for judicial scriveners who do not carefully examine whether the content of a request is intended to transfer criminal proceeds when the request is accepted.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website’s URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Business of Judicial Scriveners and Judicial Scrivener Corporations	https://www.moj.go.jp/MINJI/minji05_00607.html (Ministry of Justice)

(c) Ministry of Internal Affairs and Communications, and JFCAPLSA

From January 2018 to March 2025, the Japan Federation of Certified Administrative Procedures Legal Specialists Associations (“JFCAPLSA”) made available on its VOD training site for certified administrative procedures legal specialists and related members a training course titled “Customer Identification under the Act on Prevention of Transfer of Criminal Proceeds”, aimed at ensuring proper implementation of customer verification at the time of transaction, transaction recordkeeping, and related measures to prevent the transfer of criminal proceeds. Starting in April 2025, in light of the enforcement of the amended Act on Prevention of Transfer of Criminal Proceeds in April 2024, the course was revised and renamed “Customer Verification at the Time of Transaction under the Act on Prevention of Transfer of Criminal Proceeds – Handbook Commentary,” with videos summarizing the verification at the time of transaction and related procedures added to the training, and efforts made to ensure full awareness among all members.

Furthermore, since March 2019, JFCAPLSA has announced their obligations, such as the obligation to verify the identity at the time of transaction and the obligation to prepare verification records on the website for certified administrative procedures legal specialists, etc., in light of the survey results on the actual status of their services under the Act on Prevention of Transfer of Criminal Proceeds. It has also posted explanations about the importance of preventing ML/TF, as well as statements to increase understanding and promote measures to prevent the involvement of crime groups and terrorist groups in advance.

Furthermore, pursuant to the enforcement of the amended Act on Prevention of Transfer of Criminal Proceeds (April 1, 2024), the Ministry of Internal Affairs and Communications formulated and published the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Business of Certified Administrative Procedures Legal Specialists and Certified Administrative Procedures Legal Specialist Corporations” in April 2024 to ensure that certified administrative procedures legal specialists, etc. maintain their functions in a sound manner without being misused for ML/TF. The JFCAPLSA prepared the “Identity Verification at the Time of Transaction Handbook” and published in January 2025.

In light of the actual situation identified by the competent authorities, certified administrative procedures legal specialists, etc., should pay attention to the following matters for AML/CFT measures:

- Thoroughly verify the identity of the client at the time of transaction.
- Appropriately create and save confirmation records.
- Submit STRs.

The competent authorities are trying to improve and correct these by giving guidance to certified administrative procedures legal specialists, etc.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Business of Certified Administrative Procedures Legal Specialists and Certified Administrative Procedures Legal Specialist Corporations	https://www.soumu.go.jp/main_sosiki/jichi_gyousei/gyouseishoshi/index.html (Ministry of Internal Affairs and Communications)

(d) Financial Services Agency and Japanese Institute of Certified Public Accountants (JICPA)

The Financial Services Agency implemented the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism for Certified Public Accountants and Audit Firms" on April 1, 2024, to ensure that certified public accountants, etc. maintain their functions in a sound manner without being misused for ML/TF. In conjunction with the formulation of the guidelines, the Agency also published reference cases regarding STRs for certified public accountants, etc.

In addition, the Agency dispatched lecturers to the national training sessions organized by the JICPA to give lectures on the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism for Certified Public Accountants and Audit Firms," and contributed an article on the guidelines to the JICPA's journal.

The Japanese Institute of Certified Public Accountants (JICPA), in preparation for the smooth enforcement of the amended Act on Prevention of Transfer of Criminal Proceeds (April 1, 2024), published in July 2024 the "Sample Forms Related to the Application of the Act on Prevention of Transfer of Criminal Proceeds", which sets out templates for customer verification at the time of transaction and related procedures. The JICPA also released explanatory videos for members covering AML/CFT and other obligations required of certified public accountants, and conducted lectures on these topics during nationwide training sessions for members. In addition, the JICPA annually surveys its members regarding compliance with the Act on Prevention of Transfer of Criminal Proceeds, and uses its member website and mass email communications to share FATF-published materials on ML/TF topics, as well as various information on AML/CFT.

In light of the actual situation identified by the competent authorities, certified public accountants, etc., should pay attention to the following matters for AML/CFT measures:

- There are restrictions on specified services that certified public accountants, etc., can perform due to business restrictions under the provisions of the Certified Public Accountants Act (Act No. 103 of 1948) and the code of ethics established by JICPA.
- In the case of conducting a particular transaction (specified transaction) with a client, conduct verification at the time of transaction, create and save confirmation records and transaction records, and submit STRs.
- Refer to the business and the transactions to be provided to the client, identify and assess risks, and determine and implement mitigation measures to be taken in light of customer information and transaction details. Based on these, consider new contracts and contract reviews to avoid risks.

The competent authorities are trying to improve and correct these by giving guidance to certified public accountants, etc.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines for Anti-Money Laundering and Counter Financing of Terrorism by Certified Public Accountants and Audit Firms	https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)

(e) National Tax Agency and Japan Federation of Certified Public Tax Accountants' Associations (JFCPTAA)

The National Tax Agency conducts an annual survey of certified public tax accountants, etc., on their actual status of compliance with the Act on Prevention of Transfer of Criminal Proceeds. In addition, following the enforcement of the Act on Prevention of Transfer of Criminal Proceeds (April 1, 2024), the Agency formulated and published the "Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for Certified Public Tax Accountants and Tax Accountants' Corporation" on April 1, 2024, so that certified public tax accountants can maintain their functions in a sound manner without being misused for ML/TF.

The JFCPTAA, in collaboration with the Ministry of Finance and the National Tax Agency, produced videos as part of the training required for certified public tax accountants, etc., regarding AML/CFT measures and distributed them on its website (limited to certified public tax accountant members). The topics covered were an overview of AML/CFT measures required of Japan, verification at the time of transaction as stipulated in the amended Act on Prevention of Transfer of Criminal Proceeds, and the obligation to submit STRs. It also promotes understanding of the Act on Prevention of Transfer of Criminal Proceeds by creating checklists for verification records and revising awareness leaflets titled "AML/CFT for Certified Public Tax Accountants", which have been published on the JFCPTAA website.

In light of the actual situation identified by the competent authorities, matters that certified public tax accountants, etc., should pay attention to for AML/CFT are conduct of verification (verification at the time of transaction) and appropriate creation and retention of confirmation records and so on. The competent authorities are trying to improve and correct these by giving guidance to certified public tax accountants, etc.

[Guidelines Established by Competent Authorities]

Name of Guidelines	Website's URL
Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism for Certified Public Tax Accountants and Tax Accountants' Corporation	https://www.nta.go.jp/taxes/zeirishi/sonota/01.htm (National Tax Agency)

(iii) Assessment of Risks

Legal/accounting professionals have high expertise in law and accounting, as well as high social credibility. Transactions through their services and related affairs can be an effective means of ML/TF.

In fact, there are cases where the services of legal/accounting professionals have been misused to disguise the concealment of criminal proceeds as legitimate transactions. Considering this, it is recognized that when legal/accounting professionals conduct the following transactions on behalf of clients, the services present a risk of misuse for ML/TF.

- Acts or procedures concerning buying and selling residential lots and buildings

Real estate has high value and is easy to convert to a large amount of cash. Also, the value tends to last a long time. It is difficult to understand the financial value of real estate because various evaluations can be performed with respect to the usage value and purpose for each land. Therefore, there is a risk of misuse of real estate transactions for ML/TF, in which persons who plan to engage in ML/TF pay more than the normal price. On top of that, because sales transactions for real estate include complicated procedures, such as boundary setting and registration of the transfer of ownership, relevant expertise is indispensable. Offenders can transfer criminal proceeds more easily by performing those complicated procedures with the help of legal/accounting professionals, who possess expertise and social credibility.

- Acts or procedures concerning the establishment or merger of companies

Using a scheme involving companies and other legal persons, cooperatives, and trusts, offenders can separate themselves from the assets. This means, for example, large amounts of property can be transferred under the name of a business, and offenders can hide their beneficial owner or source of the property without difficulty. These aspects generate the risk of misuse for ML/TF. On top of that, legal/accounting professionals have expertise that is indispensable in organizing, operating, and managing companies, as well as lending social credibility. Offenders can transfer criminal proceeds more easily by establishing and operating companies with the help of legal/accounting professionals.

- Management or disposal of cash, deposits, securities, and other assets

Legal/accounting professionals have the expertise and valuable social credibility that are indispensable when storing and selling assets or using such assets to purchase other assets. When offenders manage or dispose of assets with the help of legal/accounting professionals, they can transfer criminal proceeds without difficulty.

Considering the cases where legal/accounting professionals were misused for ML, in addition to the transactions described in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, it is recognized that transactions under anonymous, fictitious or borrowed names (including those suspected to be such names) are at a higher risk based on the situation during transactions and customer attributes.

Competent authorities and self-regulatory organizations are taking the abovementioned risk-mitigation measures.

However, if these efforts differ from one legal/accounting professional to another, and legal/accounting professionals that are not taking effective risk mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, which will influence the risk for the legal/accounting industry as a whole.

2. Products and Services That Should Be Monitored Closely

(1) Casinos

Casinos are legally operated in several countries and regions outside Japan. A report published by FATF in 2009[*1] pointed out the risk of ML/TF stemming from casinos as follows:

- Casinos are a cash-intensive business, often operating 24 hours per day, with a high volume of large cash transactions taking place very quickly.
- Casinos offer various financial services (accounts, remittance, foreign exchange, etc.), but in some jurisdictions, may only be regulated as 'entertainment' venues, rather than financial institutions, and poorly regulated or unregulated for AML/CFT.
- In some jurisdictions, casino staff turnover is high, which can lead to poor education and training in AML/CFT measures.

The report also points out the ML methods and techniques in casinos as follows:

- Purchasing chips with criminal proceeds and cashing them out without using them.
- Remitting criminal proceeds from a casino account to other accounts using a chain of casinos.
- Purchasing chips from other customers with criminal proceeds.
- Exchanging large amounts of small denominations bills or coins for more manageable larger denomination bills at the cashier's desk.

Furthermore, the FATF Recommendations request each country to establish a licensing system for casino business and to require casino business operators to implement CDD, including identity verification, and check in specific cases by considering the risk of abuse of casinos for ML/TF.

In light of these requests, a licensing system for casino business was established under the Act on Development of Specified Integrated Resort Districts (Act No. 80 of 2018, hereinafter referred to as the "IR District Development Act") and the Act on Prevention of Transfer of Criminal Proceeds was amended to add casino business operators to specified business operators and to require casino business operators to verify identity and other information of customers at the time of transactions, prepare and preserve verification and transaction records, and submit STRs. Enforcement Order of the Act on Prevention of Transfer of Criminal Proceeds amended by the Order for Enforcement of the IR District Development Act (Cabinet Order No.72 of 2019) defines the following transactions as the "specified transactions" which are subject to the obligations to verify identity and other information at the time of transactions:

- Conclusion of a contract to open an account pertaining to specified fund transfer services or specified fund receipt services
- Conclusion of a specified fund loan contract
- Transactions involving the issuance of chips (transactions of issuing, granting, or receiving chips) in which the value of the chips exceeds 300,000 yen
- Receiving money pertaining to specified fund receipt services
- Transactions involving receipt or payment of casino-related money (refund of money pertaining to specified fund receipt services, receipt of payment of claims pertaining to a specified fund loan contract, or money exchange) in which the value of the transaction exceeds 300,000 yen
- Provision of premiums related to casino gaming (so-called "complimentary") in which the value of the premiums

---

*1 Vulnerabilities of Casinos and Gaming Sector (March 2009).

related to casino gaming exceeds 300,000 yen

In July 2021, the relevant enforcement regulations (Rules of the Casino Regulatory Commission No. 1 of 2021) came into force.

These IR District Development Act and its regulations, in addition to the restrictions under the Act on Prevention of Transfer of Criminal Proceeds, stipulate that the Casino Regulatory Commission must examine the Regulations on Prevention of Transfer of Criminal Proceeds prepared by the applicant during the casino business license examination process, and impose the following various obligations on casino business operators.

- To report to the Casino Regulatory Commission when the total amount involved in a transaction involves receipt or payment of cash exceeds 1 million yen on the business day
- To take measures for preventing a customer from transferring chips to other persons, receiving chips from other persons, or taking away chips from the casino gaming operation areas

In addition, in July 2022, guidelines were developed and published that establish the criteria for reviewing licenses and other dispositions related to casino businesses, as well as procedures for handling such reviews, advancing the creation of an environment where casinos are not misused for ML/TF.

Subsequently, in April 2023, based on the IR District Development Act the Minister of Land, Infrastructure, Transport, and Tourism certified the “Plan on development of specified integrated resort districts in Yumeshima, Osaka,” and procedures are underway for the establishment of IRs in Japan.

[Major Guidelines and Related Materials Issued by the Competent Authorities]

Name of Guidelines and Related Materials	Website URL(s) and Related Information
Guidelines for the Examination of Casino Business Licenses	https://www.jcrc.go.jp/policy/legal/index.html (Japan Casino Regulatory Commission)

Section 6. Low-risk Transactions

This section describes transactions with low risk.

As the principles of a risk-based approach, when risks are high, enhanced measures to manage and mitigate the risks should be taken; on the other hand, when risks are low, simplified measures may be allowed. Therefore, transactions for which simplified CDD is allowed are specified in Article 4 of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds.

1. Factors that Mitigate Risks

In light of customer and transaction attributes, payment methods, legal systems, etc., it is considered that the following transactions carry a low risk of misuse for ML/TF.

	Factors that Mitigate Risks	Why the Factors in the Left Column are Considered to Mitigate Risks
(i)	Source of funds is identified	When characteristics or ownership of a source of funds are clear, it is difficult to misuse them for ML/TF.
(ii)	The customer, etc., is the national government or a local public entity	Transactions with the national government or a local public entity are carried out by national officers, etc. under powers given by laws, internal control systems, etc. As the process and nature of such transactions are highly transparent, and the sources/destinations of funds is clear, it is difficult to misuse them for ML/TF.
(iii)	Customers, etc., are limited under laws and regulations.	In some transactions, customers or beneficiaries are limited by laws, etc. It is difficult for those who attempt ML/TF to participate in such transactions, so it is difficult to misuse them for ML/TF.
(iv)	The transaction process is supervised by the national government, etc. based on laws, etc.	Transactions in which notification to or approval by the national government etc. is required are supervised by the national government, etc., so it is difficult to misuse them for ML/TF.
(v)	It is difficult to disguise the actual status of legal persons, etc.	In general, services that provide legal persons, etc., with an address, facilities, means of communication for business/management present risks of being misused for ML/TF because such services may create a fictitious or exaggerated appearance of business credibility, business scale, etc. However, once it becomes problematic for those services to disguise the actual status of their legal person, etc., it, in turn, becomes difficult to misuse them for ML/TF.
(vi)	Minimal or no fund-accumulation features	Investment in products or services with no or minimal fund-accumulation features is inefficient for ML/TF.
(vii)	The transaction amount is less than the regulatory threshold	Transactions below the regulatory threshold are inefficient for ML/TF*[1].
(viii)	Customer identification measures are secured by laws, etc.	In some transactions, customers or beneficiaries are verified under laws, etc., or are limited to persons who, conforming with business regulations, obtained a business license from the national government, etc. Thus, customers' identities are clear, and fund traceability is secured in such transactions.

*[1] In the FATF Recommendations and Interpretative Notes etc., the FATF also sets out transaction amounts that are the thresholds for CDD measures. However, if one transaction above the threshold is divided into several transactions and the amount of each divided transaction falls below the threshold, such an action (structuring) is to avoid regulation, and has a high risk of being misused for ML/TF. The Act on Prevention of Transfer of Criminal Proceeds and the Enforcement Order of the Act on Prevention of Transfer of Criminal Proceeds provide that when specified business operators conduct two or more transactions (receipt or payment of cash, withdrawal of deposit/savings, foreign currency exchange, sales of precious metal, etc.) with the same customer at the same time or continuously, and the transactions obviously represent a divided single transaction, the separate transactions should be regarded as a single transaction.

2. Types of Low-risk Transactions

Specific transactions that have factors to mitigate risks described in 1. above are as follows. However, even if a transaction falls under the category shown below, if it is a suspicious transaction or one that requires special attention in CDD, it is not recognized as a low-risk transaction[*1].

	Specific Types of Low-risk Transactions		Reasons Listed in 1. Above
1	Certain Transactions in Money Trusts, etc.	Transactions conducted for the purpose of managing assets to be returned to the beneficiaries as set forth in Article 4, paragraph (1), item (i) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds (money trusts), etc.	(i), (iii), (iv), (viii)
2	Conclusion, etc. of Insurance Contracts	Conclusion of insurance contracts set forth in Article 4, paragraph (1), item (ii) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds ((a): insurance contracts under which maturity proceeds, etc., are not paid; (b): insurance contracts under which the sum of return premiums is less than 80% of the sum of insurance premiums paid), etc.	(vi)
3	Payment of Maturity Proceeds, etc.	Payment of maturity proceeds of insurance contracts set forth in Article 4, paragraph (1), item (iii), (a) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds, under which the sum of return premiums is less than 80% of the sum of insurance premiums paid	(vi)
		Payment of maturity proceeds of qualified retirement pension contracts or franchise insurance contracts,[*2] etc., as set forth in Article 4, paragraph (1), item (iii), (b) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(i), (iii), (iv), (viii)
4	Transactions Carried out in a Securities Market (exchange), etc.	Sale and purchase of securities conducted on a securities market (exchange), etc.[*3] as set forth in Article 4, paragraph (1), item (iv) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(iii), (viii)
5	Transactions of Government Bonds, etc., that are Settled by an Account Transfer at the Bank of Japan	Book-entry transfer of Japanese government bonds conducted at the Bank of Japan, etc., as set forth in Article 4, paragraph (1), item (v) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(iii), (viii)
6	Certain Transactions concerning the Loan of Money, etc.	Money lending or borrowing for which book-entry transfer is conducted at the Bank of Japan as set forth in Article 4, paragraph (1), item (vi), (a) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(iii), (viii)
		Insurance contracts under which the sum of return premiums is less than 80% of the sum of insurance premiums paid as set forth in Article 4,	(i), (iii), (iv), (vi)

[*1] In the Act on Prevention of Transfer of Criminal Proceeds and the Enforcement Order of the Act on Prevention of Transfer of Criminal Proceeds, transactions for which simplified CDD is allowed as prescribed by the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds are excluded from specified transactions that requires verifications at the time of transactions. However, such transactions are not excluded from specified businesses that requires the preparation and preservation of transaction records and submission of STRs, and they are subject to the prescribed CDD. In addition, the Act and the Enforcement Order stipulate that if a transaction is suspicious or requires special attention when implementing CDD, such transaction is considered to be a specified transaction and will be subject to verification at the time of transaction, even if the transaction is a transaction for which simplified CDD is allowed.

[*2] In group insurance, the amount that is deducted from the salary of employees is used for premiums.

[*3] Financial instruments exchange markets prescribed in Article 2, paragraph (17) of the Financial Instruments and Exchange Act or over-the-counter securities markets prescribed in Article 67, paragraph (2) of the same Act, or foreign markets (only in jurisdictions designated by the Financial Services Agency Commissioner) where sales and purchase of securities equivalent thereto or Foreign Market Transaction of Derivatives prescribed in Article 2, paragraph (23) of the same Act is carried out.

		paragraph (1), item (vi), (b) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	
		Individual Credit*[1], etc. set forth in Article 4, paragraph (1), item (vi), (c) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(viii)
7	Certain Transactions in Cash, etc.	Transactions for providing certificates or interest coupons of public and corporate bonds without the owner's name when a volume of transactions exceeds 2 million yen as set forth in Article 4, paragraph (1), item (vii), (a) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(i), (viii)
		Payment or delivery of money or goods to the national or a local government as set forth in Article 4, paragraph (1), item (vii), (b) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(viii)
		Payment of charges for electricity, gas, or water as set forth in Article 4, paragraph (1), item (vii), (c) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(viii)
		Payment of enrollment fees and tuition, etc., to elementary schools, junior high schools, high schools, and colleges, etc., as set forth in Article 4, paragraph (1), item (vii), (d) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(viii)
		Exchange transactions of not more than 2 million yen for depositing and withdrawing funds as set forth in Article 4, paragraph (1), item (vii), (e) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(vii), (viii)
		Transactions for receiving or paying the price of goods of not more than 2 million yen in cash that involve exchange transactions, for which verification of identity and other information of a payer at the time of transaction is conducted by a payee in the same manner as specified business operators as set forth in Article 4, paragraph (1), item (vii), (f) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(vii), (viii)
8	Opening a Special Account under the Act on Book-Entry Transfer of Corporate Bonds and Shares*[2]	Opening special accounts under the Act on Book-Entry Transfer of Corporate Bonds and Shares as set forth in Article 4, paragraph (1), item (viii) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(iii), (viii)
9	Transactions through SWIFT	Transactions for which verification is conducted or payment instruction is provided between specified business operators, etc., through SWIFT as set forth in Article 4, paragraph (1), item (ix) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds*[3]	(iii), (viii)

*[1] Individual credit is a type of transaction. When purchasers buy products from sellers, purchasers do not involve cards, etc. Instead, an intermediary provides the amount equivalent to the product price to the seller according to the contract with purchasers and sellers, and purchasers make payment of the price according to a certain fixed method to the intermediary later.

*[2] Act No. 75 of 2001

*[3] Transactions whose customer is a specified business operator and the Bank of Japan as well as a person equivalent thereto who has his/her head office or principal office in a foreign country (hereinafter referred to as a "foreign specified business operator" in this item) that uses a specified communications method (an international communications method used between a specified business operator, the Bank of Japan, and a foreign specified business operator, designated by the Commissioner of the Financial Services Agency as which necessary measures are taken to identify the specified business operator, the Bank of Japan, and the foreign specified business operator that is communicating with) for which verification is made or settlement is directed through the said specified communications method. SWIFT (Society for Worldwide Interbank Financial Telecommunication) is designated as a specified communication method as set forth Article 4, paragraph (1), item (ix) of the Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds (Public Notice of the Financial Services Agency No. 11 of 2008).

10	Specified Transactions in Financial Leasing Contracts	Financial leasing transactions in which an amount of rental fee received by a lessor at one time is not more than 100,000 yen as set forth in Article 4, paragraph (1), item (x) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(vii)
11	Buying and Selling Precious Metals and Stones, etc., in Which the Payment is Made through Methods Other Than Cash	Transactions in which precious metals and stones, etc., in an amount equal to or above 2 million yen are sold and purchased by any payment method other than cash as set forth in Article 4, paragraph (1), item (xi) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(viii)
12	Certain Transactions with Telephone Receiving Services	Certain transactions with telephone receiving services as set forth in Article 4, paragraph (1), item (xii) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds ((a): telephone receiving services contracts that include provisions clearly indicating to a third party that the services are telephone receiving services; (b): contracts for call center services, etc.*[1])	(v)
13	Transactions with the National Government, etc., as a Customer	Transactions conducted by the national or a local government with the authority under laws and regulations as set forth in Article 4, paragraph (1), item (xiii) (a) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(i), (ii), (iii), (iv), (viii)
		Transactions conducted by a bankruptcy trustee, etc., with the authority under laws and regulations as set forth in Article 4, paragraph (1), item (xiii) (b) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(i), (iii), (iv), (viii)
		Transactions conducted by a specified business operator with its subsidiary, etc., as a customer as set forth in Article 4, paragraph (1), item (xiii) (c) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(i), (viii)
14	Specific Transactions in Agent Work, etc., for Specified Mandated Acts by Judicial Scriveners, etc.*[2]	Conclusion of contracts for voluntarily appointed guardians as set forth in Article 4, paragraph (3), item (i) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(iv), (viii)
		Transactions conducted by the national government, etc., with the authority under laws and regulations, or transactions conducted by a bankruptcy trustee with the authority under laws and regulations as set forth in Article 4, paragraph (3), item (ii) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(i), (iv), (viii) and (ii) or (iii)

*[1] Businesses that take telephone calls (including telecommunications by facsimile devices) to provide explanations about or consultation on goods, rights, or services, or to receive applications or to conclude contracts for the goods, rights or services. Specific examples of call center services include reception of requests for information and inquiries, customer centers, help desks, support centers, consumer consultation desks, maintenance centers, order centers, etc.

*[2] Regarding agent work, etc. for specified mandated acts pertaining to the management or disposition of property listed in item 3 of the middle column of the row of persons listed in Article 2, paragraph (2), item (xlvi) in the attachment to the Act on Prevention of Transfer of Criminal Proceeds, cases where the value of the said property is no more than 2 million yen are excepted.

Section 7. Risk Related to Terrorist Financing

The threat of international terrorism remains high, with terrorist attacks occurring in various parts of the world. Additionally, there are concerns that foreign fighters[*1] who participated in battles in Iraq and Syria may commit acts of terrorism after returning to their home countries or moving to third countries. As the threat of terrorism has spread across borders, it is essential that countries cooperate with each other in implementing countermeasures against terrorist financing. In Japan as well, the risks related to terrorist financing have become increasingly complex due to the diversification of targets, funding channels, and methods of transfer. Accordingly, comprehensive analysis and responses based on international standards are required.

This report assesses the risk related to terrorist financing from the following perspectives, taking into account the FATF Recommendations and their Interpretive Notes, various reports published by the FATF, and measures implemented under Japan's Act on Prevention of Transfer of Criminal Proceeds.

Threats	Terrorist groups such as ISIL, AQ, and other Islamic extremists and their financiers
Vulnerabilities	legal and illegal sources and methods of terrorist financing

After comprehensively considering the above, including an assessment of potential impacts on Japan, Islamic extremists such as ISIL and AQ, foreign fighters, and individuals believed to have become extremists under the influence of online propaganda by Islamic extremist organizations were identified as high-risk attributes. In this report, individuals with these attributes are collectively referred to as "Islamic extremists."

1. Factors that Increase Risks

(1) International Terrorism Situation and Threat Targeting Japan

The threat of terrorist financing arises from the continued activities of terrorist organizations or their supporters, who require and seek to raise funds. In the international community, including Japan, activities of Islamic extremists as described below, have been observed and are positioned as major threats in the context of terrorist financing risks.

○ Threats posed by Islamic extremists

By March 2019, ISIL had lost all the territories it controlled in Iraq and Syria. However, affiliated organizations in various regions that claim to be "provinces" of ISIL have expressed their loyalty to the fifth leader Abu Hafs al-Hashimi al-Qurashi, who assumed as the role of leader in August 2023. The following points have been observed regarding ISIL:

- It has consistently called for acts of terrorism against Western and other countries participating in the "Global Coalition to Counter ISIL" as retaliation for their military interventions in Iraq and Syria.
- There is a risk that many of the foreign fighters and their families will leave the former ISIL-controlled territories and travel to their home countries or third countries to carry out terrorist attacks.
- Some of those who remain in the former ISIL-controlled territories are still active without being detained.
- There is a possibility that further radicalization will occur in detention facilities or refugee camps.

Furthermore, in Syria, in December 2024, anti-government forces centered on HTS overthrew the Assad regime and established an interim government with the HTS leader as president. However, the situation remains

[*1] Persons who travel to countries/regions other than the country of residence or nationality for the purpose of preparing, planning, or carrying out terrorist acts, or to receive training for such purposes.

unstable, and there are concerns that international terrorist organizations, including ISIL, may seek to carry out terrorist acts taking advantage of this instability.

In recent years, AQ has faced losses of group leadership due to the killing of senior members of affiliated organizations in counterterrorism operations by various countries, and in July 2022, for example, AQ leader Ayman al-Zawahiri was killed in a US operation. However, AQ-affiliated groups operating in the Middle East and Africa continue to carry out attacks targeting local government entities. The impact of Zawahiri's death on these affiliated organizations is believed to be limited.

In addition, following the terrorist attacks on Israel by Palestinian armed groups such as Hamas in October 2023 and the subsequent armed conflict, ISIL, AQ and their affiliates and supporters have been calling for terrorist attacks against Israel and Western interests, and terrorist incidents believed to be related to this situation have occurred in various countries. As such, it can be said that the threat of international terrorism remains high.

Furthermore, in Afghanistan, where Kabul, the capital,was seized by the Taliban in August 2021, the security situation remains unstable, including terrorist attacks carried out by ISIL-K*[1], which is based in the country and surrounding areas. Links between the Taliban and AQ have been highlighted, raising concerns that the threat posed by AQ may be resurging.

○ Threat of terrorism targeting Japan

No Japanese national or person residing in Japan has been included in the list of the targets of asset freezing and other measures pursuant to UNSCR 1267 and succeeding related resolutions and UNSCR 1373, as well as Cabinet Decisions. To date, no terrorist activity by terrorists designated by the United Nations Security Council has been confirmed in Japan.

However, in Japan, there are people claiming to be in touch with persons affiliated with ISIL and those who express their support for ISIL on the Internet, which indicates that the network of Islamic extremist organizations that are loosely connected through extremism is affecting Japan. Therefore, the possibility that terrorism could be carried out in Japan by those influenced by the extremist ideologies of ISIL, AQ, and their affiliated organization cannot be ruled out, and continued vigilance remains necessary.

Table 112: Number of International Terrorism Cases

Item/year	2021	2022	2023
Number of cases	8,357	7,351	7,382
Number of deaths	23,712	21,957	21,596

Note: Based on the U.S. Department of State "Annex of Statistical Information2023"

Table 113: Major Terrorism Cases in 2024

Date	Case
January 3	Suicide bombing terrorist incident in Kerman, Iran
March 22	Terrorist attack in Moscow, Russia

*[1] Abbreviation of Islamic State in Iraq and the Levant-Khorasan associated with ISIL.

August 7	Attempted terrorist attack targeting a concert venue in Vienna, Austria

Note: Excerpt from the National Police Agency's "The White Paper on Police 2025"

(2) Characteristics

Based on the observations and analyses of the FATF and the Egmont Group, the characteristics of terrorist financing are as follows.

○ Diversity and concealment of the sources of funds

Terrorist financing may be obtained through taxation imposed by terrorist organizations in transactions conducted in regions under their control, crimes such as drug smuggling, fraud, abduction for ransom, or monetary assistance provided to foreign fighters by their families. It may also be obtained through activities disguised as legitimate transactions by organizations and companies.

○ Difficulty of detection due to small amount and fragmented transaction types

Some transactions related to terrorist financing may be conducted through cross-border remittances to financial institutions located in the regions under terrorist organizations' control. However, as such transactions may be smaller in value than transactions related to ML, there is a risk that they may become invisible among the numerous transactions handled routinely by business operators.

○ Characteristics of the recipient and intermediary locations

Money intended for terrorist financing is sent to Iraq, Syria, and Somalia, among others. However, in some cases, money is transferred through Turkey or other neighboring countries instead of sending directly to these countries.

○ Use of Cryptoassets

ISIL-K, through its affiliated media outlet *Voice of Khurasan*, has called for funding using Monero, a type of cryptoassets, and has actually raised funds in the tens of thousands of U.S. dollars. This indicates a shift in fundraising methods from traditional criminal activities such as ransom kidnappings to donations from ISIL-K supporters using cryptoassets.

○ Use of Social Media

In terrorist financing and related activities, the use of social media, crowdfunding platforms, and mobile applications has been increasing. At the same time, videos are used to promote extremist ideology and solicit donations.

○ Traditional Methods

ISIL is reported to continue widely using traditional methods, such as hawala[*1] and direct cash transfers, and to make use of various financial hubs as transfer routes.

(3) Domestic Cases

Although there have been no cleared cases in Japan in relation to terrorist financing, there have been cases suggesting resonance with the ideology of Islamic extremists among foreign residents in Japan, as well as cases in which domestic groups are suspected of providing financial support to international terrorist organizations, as outlined below.

[*1] Refers to an informal value transfer system commonly used in the Middle East, North Africa, and the Indian subcontinent.

[Case 1] Unauthorized exports by individuals believed to have been influenced by the ideology of Islamic extremists

Images from which sympathy for Islamic extremism can be perceived and videos related to the production of explosives were stored in computers owned by two Indonesians in Japan who were arrested for violating the FEFTA (unauthorized export) because they exported rifle scopes to Indonesia without a permit even though it is necessary to obtain a permit from the Minister of Economy, Trade and Industry to export them.

[Case 2] Fund transfers using illegally opened accounts

A company executive was arrested for opening an account for a third party and stealing a cash card. It was found out that there were remittances to the account from an entity in Japan, which is considered to support a member of the Japanese Red Army[*1] placed on the international wanted list, and almost all of the money was withdrawn in a foreign country.

(4) Cases in foreign countries

In addition to domestic cases, the following are examples of foreign incidents revealed by law enforcement agencies and media in various countries, provided to deepen understanding of the actual situation and typical methods of terrorist financing.

[Case 1] Use of Cryptoassets for Terrorist Financing (South Korea)

Uzbek national A was sentenced to one year and six months' imprisonment for supporting KTJ[*2], an AQ-affiliated organization. A received a request via Telegram from KTJ to provide funds and, despite knowing that KTJ was a terrorist organization, provided cryptoassets and other assets equivalent to 4 million won (approximately USD 2,900) to two KTJ members over 20 occasions.

[Case 2] Remittance of Terrorist Funds through an Employer (Singapore)

Indonesian national A deceived his employer into believing that his salary was being remitted to an account held by his relative, and caused the employer to transfer approximately SGD 1,200 (approximately USD 930) over five occasions to an account held by supporters of ISIL and others.

[Case 3] Transfer of Funds from Social Security Account (Indonesia)

Indonesian national A transferred up to 60 million Indonesian rupiah (approximately USD 4,000) to individual B, his brother who had already joined ISIL in Syria, and to individual C. A is alleged to have withdrawn cash from B's social security insurance account using B's identification documents and to have remitted the funds through an intermediary located in Syria.

[Case 4] Transfer of Terrorist Funds through Legitimate Money Transfer Service Providers (Australia)

Australian national A remitted USD 18,000 to Pakistan and Turkey in order to support an individual who had traveled from Pakistan to Syria with the intention of joining ISIL as a foreign fighter. The transferred funds are

[*1] The Japanese Red Army has carried out numerous international terrorist incidents in the past, and seven fugitive members remain internationally wanted. Efforts are being advanced to apprehend these fugitives and to clarify the organization's activities.
[*2] Abbreviation for Khatiba al-Tawhid wal-Jihad.

suspected to have been provided, through an intermediary in Turkey, to Australian ISIL fighter B. The group involved in these transfers is reported to have used international money transfer services to remit terrorist funds.

[Case 5] Facilitation of Cryptoassets Usage for Terrorist Financing (United States)

An American, Person A, shared methods on social media for concealing ISIL funding using Bitcoin and offering assistance to ISIL sympathizers planning to travel to Syria, thereby providing advice to ISIL and its supporters. Person A also admitted to supporting the travel of a US-resident minor with intentions of joining ISIL for combat purposes to Syria. Additionally, Person A's social media account had more than 4,000 followers and was used as a platform for supporting ISIL through over 7,000 posts. In particular, Person A used the account to share explanations about Bitcoin and how its system works, introduce new tools for anonymizing Bitcoin users, and provide links to his own article titled *"Bitcoin wa' Sadaqat al-Jihad (Bitcoin and the charity of Jihad)"*. Through these activities, Person A used the same account to post about expanding methods of funding ISIL using online currencies like Bitcoin, as well as establishing a system for donations to ISIL through secure means, all shared on social media.

[Case 6] Travel to Conflict-affected Area with Loan from Banks (Malaysia)

Several Malaysian ISIL supporters obtained funds to join ISIL by using personal loans from banks. The report said that more than five ISIL supporters, including a former trainer in the Malaysian military training program, planned to travel by using loans from banks. Although the highest amount of loan was 30,000 USD, the credit standing of young radicals in their twenties is still low, so they applied for a loan of 5,000 Ringgits (about 1,400 USD). Two other radicals were planning to use their funds to travel to Iraq or Syria, procure goods, and pay for living expenses in Iraq or Syria.

2. Trends of STRs

(1) Key Points to Note When Submitting STRs

When submitting STRs related to terrorist financing, in addition to the general considerations applicable to ML, it is necessary to take into account the characteristics specific to terrorist financing and pay attention to the following points.

[Customer Attributes]

Identification matters (such as name and date of birth) and aliases, etc., of persons subject to asset freezing under the FEFTA and the International Terrorist Asset-Freezing Act.

[Countries/Regions Involved in Transaction]

Whether the remittance destination or remittance origin is countries/regions where terrorist organizations operate, or a neighboring countries/regions thereof.

In addition, taking into consideration the following points indicated by the FATF, it should be noted that the risk of terrorist financing may exist not only in countries/regions adjacent to conflict areas such as Iraq and Syria, but also in other countries/regions.

- Technological advances, such as social media and new payment methods, have created vulnerabilities in measures to combat terrorist financing.
- Even in countries with a low risk of terrorism, there remains a possibility of exposure to terrorist financing

risks, for example where funds are raised or stored domestically, or transferred through such countries.
[Transaction Types]
● Even if the stated purpose of the remittance is a donation or similar payment, whether the recipient is an organization or individual whose actual activities lack transparency. ● Whether, after the remittance, there is an immediate cash withdrawal or an immediate transfer to a different account.

(2) Trends Observed in Reported Cases

With regard to transactions related to terrorist financing, specified business operators have been proactively submitting STRs, and the reports exhibit the following characteristics.

[Reports Submitted due to Similarities in Names]
The report is submitted on the grounds that the customer’s name is similar to that of a person subject to asset freezing measures or a person reported as being connected to terrorism.
[Reports Submitted Based on the Customer Attributes and Transaction Details]
The report is submitted by a specified business operator on the grounds that, based on the customer attributes, transaction types, and other factors, there is a suspicion of terrorist financing.
[A High Proportion of Cross-Border Transaction]
Looking at the nature of the reported transactions, the majority involve cross-border transactions, and the countries/regions concerned are often in Asia and the Middle East
[Repeated Cash Withdrawal Behavior]
Among the STRs, there are cases where transactions involving multiple large cash withdrawals using a debit card in a Middle Eastern country, combined with the customer attributes, were assessed as potentially related to terrorist financing and were therefore reported.

These transaction types are consistent with the typical indicators of terrorist financing identified by the FATF and the Egmont Group, indicating that potential risks also exist in Japan.

Specified business operators are therefore expected to continue enhancing transaction monitoring and the judgment for submitting reports on a risk-based approach, taking the above points into consideration.

3 Measures to Mitigate Risks

(1) Statutory measures

○ Act on Prevention of Transfer of Criminal Proceeds and Act on Punishment of Organized Crimes

● The Act on Punishment of Organized Crimes sets forth that terrorist financing and other crimes are predicate offences of ML. Terrorist funds may be regarded as criminal proceeds under the Act.

● It stipulates that any transaction of assets suspected to be terrorist funding is subject to being reported as an STR under the Act on Prevention of Transfer of Criminal Proceeds.

● Each time the list of groups subject to asset freezing and other countermeasures, pursuant to United Nations Security Council resolutions (No. 1267 and its succeeding resolutions and No. 1373) and Cabinet approval is updated, the National Police Agency urges specified business operators through competent authorities to fulfill their obligation to perform verification at the time of transactions in accordance with the Act on Prevention of

Transfer of Criminal Proceeds and diligently submit STRs.

○ Act on Punishment of Terrorist Financing

- It was established for the purpose of developing the necessary domestic laws to respond to international requests to implement the measures to prevent terrorist financing such as International Convention for the Suppression of the Financing of Terrorism.
- It defines certain offences, including murder or aircraft hijacking, performed for the purpose of threatening the general public or national, local, or foreign governments as "act of public intimidation." It also defines offences that are subject to the crime of financing as "specified act."
- It includes provisions to punish certain acts, such as when a person who intends to engage in an act of public intimidation or specified act (hereinafter referred to as "Act of Public Intimidation, etc.") forces someone else to provide funds for such act or other benefits (including lands, buildings, goods, services, and other benefits other than funds, and hereinafter referred to as "Funds, etc.") that support such act, or when someone provides Funds, etc. to a person who intends to engage in an Act of Public Intimidation, etc., or when someone provides Funds, etc. for collaborators who intend to provide Funds, etc. for a person who intends to engage in an act of public intimidation, etc. (Based on United Nations Security Council Resolution 1267 and other measures to address the movement of illicit funds internationally, promulgated in December 2022, the law partially amending the Act on Special Measures Concerning the Freezing of Assets of International Terrorists and Others, as implemented by Japan, raised the statutory penalties.)

○ FEFTA

- With respect to international transactions, in response to the United Nations Security Council resolutions (No. 1267 and its succeeding resolutions and No. 1373) and Cabinet approval on asset freezing and other measures, simultaneous asset freezing by G7 and various other asset-freezing measures have been implemented against individuals and groups subject to such measures in accordance with the FEFTA.
- As of August 28, 2025, 418 individuals and 122 entities have been designated as such individuals and entities. Payments to these individuals and entities, capital transactions (deposit transactions, trust transactions, and contracts for a loan of money) with these individuals and entities are conducted under a permission system, and measures such as asset freezing take place through refusing permission.

○ International Terrorist Asset-Freezing Act

- With respect to domestic transactions, in response to the United Nations Security Council resolutions (No. 1267 and its succeeding resolutions and No. 1373) and Cabinet approval on asset freezing and other measures, measures such as freezing assets have been taken against designated individuals and entities.
- As of August 28, 2025, the names of 418 individuals and 122 entities have been publicly announced as international terrorists subject to measures such as freezing assets. Such individuals and entities are required to obtain permission from prefectural public safety commissions when they conduct certain actions, such as receiving a donation of money.
- Prefectural public safety commissions may order publicly announced international terrorists to submit parts of the assets that they hold and provisionally confiscate those assets.

(2) Other Measures

○ In December 2022, under the leadership of the Prime Minister in the Ministerial Meeting on Crime Control, the Strategy to Make Japan “the Safest Country in the World” (2022) was established. This Strategy includes strengthening anti-money laundering, counter-terrorist financing, and proliferation financing, in line with the recommendations of the FATF.

○ The Police have been promoting anti-terrorist measures from both prevention and response aspects, including:

- Information collection and analysis and thorough investigation
- Enhanced border security in collaboration with relevant agencies such as the Immigration Services Agency and Customs
- Promotion of anti-terrorist cooperation between government and private entities
- Enhanced protection of critical public facilities

○ In December 2022, the National Police Agency and the Financial Services Agency conducted a briefing session for financial institutions and relevant organizations on countermeasures against terrorist financing, with the aim of enhancing their understanding of the risks associated with terrorist financing.

○ Awareness-raising on measures to prevent terrorist financing for non-profit organizations

The Cabinet Office has developed the “Guidance on Measures to Prevent the Financing of Terrorism by corporations engaging in specified non-profit activities (hereinafter referred to as “CESNAs”)” which outlines the actions CESNAs should take to prevent their misuse for terrorist financing. This guidance is continuously updated in light of international developments and requests based on FATF Recommendation 8, with the latest version published in June 2025. Although it is designed specifically for CESNAs, the guidance also serves as a reference for non-profit organizations in general, promoting transparency of funds and the establishment of appropriate risk management systems, and is utilized as part of awareness-raising and support efforts for relevant stakeholders.

4 Assessment of Risks

In Japan, legal measures related to terrorist financing have been established, and compared to other countries, the risk of terrorist financing is assessed to be relatively low.

In fact, no person of Japanese nationality or residency has been included in the list of persons against whom asset freezing measures are implemented pursuant to the United Nations Security Council resolutions (No. 1267 and succeeding resolutions as well as No. 1373) and Cabinet approval. There have been no terrorist acts carried out in Japan by the terrorists designated by the United Nations Security Council so far.

However, the FATF pointed out in its report[*1] released in 2019 that even when there have not been any cases of terrorist attacks or terrorist financing in a country, that fact does not immediately lead to the conclusion that the risk of terrorist financing is low; the possibility of funds being collected in that country and being remitted abroad should not be excluded.

In light of the matters related to the threat of terrorism to Japan and the threat of and vulnerability to terrorist financing that have been pointed out internationally, the following activities should be recognized as concerns:

- Members of Islamic extremist and other terrorist groups hide themselves in communities of foreigners and misuse

---

[*1] Terrorist Financing Risk Assessment Guidance (July 2019)

the communities for fundraising.

- Foreign fighters engage in fundraising and other activities.
- Persons who travel to conflict areas may become the parties conducting terrorist financing.
- Terrorist financing may be provided through transactions disguised as legitimate ones conducted by Japanese organizations and companies.
- Products and services provided by specified business operators (including cryptoassets transfer) may be misused without being monitored by the business operators.

In light of these circumstances, it is acknowledged that there is a particularly high risk of terrorist financing when conducting transactions suspected to involve Islamic extremists.

Moreover, the act of preparing for terrorism is highly secretive, and most terrorism-related information collected is fragmented, so it is still crucial to accumulate further information and conduct a continuous and comprehensive analysis in light of the abovementioned risks.

[Topic] Risk of Abuse of Nonprofit Organizations for TF

The FATF, in Recommendation 8, calls its member countries to implement measures based on a risk-based approach to prevent nonprofit organizations from being abused by terrorists or other illicit actors. This topic first organizes the threats and vulnerabilities related to terrorist financing risks for nonprofit organizations in Japan, based on international assessment standards and risk perceptions. It then analyzes the actual conditions and institutional responses for each type of non-profit organization in Japan, and ultimately conducts a risk assessment.

1 Key Characteristics of Nonprofit Organizations*1 Regarding the Risk of Terrorist Financing

Nonprofit organizations in Japan are a collective term for organizations that do not aim to distribute profits to their members and engage in various social contribution activities. Individual laws, such as the Act on Promotion of Specified Nonprofit Activities (Act No. 7 of 1998; hereinafter referred to as "APSNA") and the Act on Authorization of Public Interest Incorporated Associations and Public Interest Incorporated Foundations (Act No. 49 of 2006), regulate their establishment and management.

According to the FATF Recommendations and Their Interpretive Notes, not all nonprofit organizations are considered to carry a uniformly high risk. Since the risk level varies depending on the nature of activities, regions where they operate, and the structure of their transactions, the responses are required that take into account the threat and vulnerability of individual organizations*2.

(1) Inherent Vulnerabilities of Nonprofit Organizations

As a background for the potential abuse of nonprofit organizations for terrorist financing, the following structural vulnerabilities have been identified.

- Nonprofit organizations, generally having gained societal trust, tend to handle intensively amounts of cash using various funding sources.
- Organizations operating in conflict areas or their surroundings may, as a result, provide a financial transaction framework that could be used to support the activities of terrorist organizations.
- There are many instances where the entities raising funds for activities differ from those disbursing them, creating a structure in which the ultimate use of funds tends to lack transparency

(2) The Threat of Funding through Nonprofit Organizations

While there have been no confirmed cases of nonprofit organizations being abused for terrorist financing within Japan, nonprofit organizations operating overseas may face potential threats from terrorist organizations active in those regions.

Specifically, foreign cases and FATF typology analyses have highlighted the following modus operandi.

- Terrorist organizations and their supporters establish nonprofit organizations under the guise of charitable activities, raise funds and provide them as support payments to terrorists or their families.
- Terrorist associates may infiltrate legitimate nonprofit organizations, and, through their legitimate financial transactions, funnel money to terrorist organizations located in conflict zones.
- Legitimate organizations may unintentionally provide funds to other nonprofit organizations that have links to terrorist groups abroad, which may then be used as terrorist financing.

Documents related to FATF Recommendation 8 identify the following three types of abuse:

(a) Terrorist organizations masquerading as legitimate organizations

(b) Legitimate organizations being used as transaction channels

---

*1 In light of the fact that FATF defines that "a nonprofit organization is a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social, fraternal or other purposes, or for the carrying out of other types of good works," the "Strategic Policy towards Promoting AML/CFT/CPF" of Japan lists corporations engaging in specified nonprofit activities (CESNA), public interest corporations, social welfare corporations, medical corporations, incorporated educational institutions and religious corporations as nonprofit organizations.

*2 The FATF notes that measures to protect non-profit organizations from the misuse for terrorist financing must not hinder or prevent them from carrying out legitimate

(c) Legitimate funds being diverted to terrorist organizations

The methods of funding through nonprofit organizations are recognized internationally as a serious threat. United Nations Security Council Resolution 2462, adopted in March 2019, expressed serious concern regarding acts in which terrorists or related actors exploit legitimate businesses or nonprofit organizations to raise or transfer funds. In addition, the emergence of new financial instruments, such as cryptoassets, has raised concerns that funds transferred through such organizations may become difficult to trace.

2 Nonprofit Organizations in Japan

Nonprofit organizations in Japan have different legal frameworks and activity characteristics depending on their corporate type. The competent authorities conduct supervision and guidance based on each institutional framework and, taking into account the results of risk assessments, carry out monitoring based on a risk-based approach. The following topic organizes the institutional characteristics of each type of organization, their vulnerabilities related to terrorist financing risks, and measures taken to mitigate those risks, with the aim of understanding the actual risk structure of nonprofit organizations in Japan.

(1) Corporations Engaging in Specified Non-profit Activities (CESNAs) <Jurisdiction: Cabinet Office>

(i) Characteristics

A corporation engaging in specified non-profit activities(hereafter referred to as “CESNAs”) is an entity primarily focused on conducting specified nonprofit activities based on the Act on Promotion of Specified Nonprofit Activities (hereinafter referred to as the “APSNA”). “Specified nonprofit activities” are those falling under the 20 categories of activities listed in APSNA, aiming to contribute to enhancing the interest of many and unspecified persons. The areas of activity for CESNAs include, for example, “activities aimed at enhancing healthcare, medical care, and welfare,” “protecting human rights or promoting peace,” and “engaging in international cooperation.”

When establishing a CESNA, the required documents to the competent authority include the articles of incorporation detailing the type of the non-profit activities it engages in and type of the business pertaining to the non-profit activities, a list of officers, documents stating the names of its members, a document stating the purpose of incorporation, business plans. This application undergoes an examination, and certification is granted upon approval.

As of the end of July 2025, there are 49,252 CESNAs.

(ii) The vulnerabilities of CESNAs Related to Terrorist Financing

The following points can be cited as structural vulnerabilities that could make CESNAs susceptible to abuse for terrorist financing.

● Operating in regions exposed to the threat of terrorism or in conflict areas

Some CESNAs operate in areas where terrorist acts occur, including their vicinity, for humanitarian reasons. The operational areas of these corporations may overlap with terrorist active zones, and the people they assist may be in close proximity to terrorists. These circumstances create a risk that funds or supplies intended for support could be misappropriated.

● Handling of substantial amounts of funds and use of cash abroad

Some CESNAs receive substantial donations or grants and provide support through foreign remittances or the physical transfer of cash. Such cash transactions and transfers are highly anonymous, making it difficult to trace the flow of funds and increasing the risk of misuse.

● Difficulty in identifying stakeholders due to collaboration with foreign partners and the utilization of volunteers

When CESNAs expand their activities abroad, they frequently collaborate with local partners, and many volunteers participate in their operations. In such situations, the identities of stakeholders may not be adequately verified, creating a risk of involvement by terrorist organizations and their supporters.

● Existence of organizations with unclear operational activities

A certain number of organizations that are so-called dormant, or whose business reports indicate "no activity record" or "no expenditure during the fiscal year." Such corporations carry a risk of being misused in name only by terrorist organizations or other illicit actors.

(iii) Measures to Mitigate Risks

Regarding the risk of terrorist financing by CESNAs, APSNA provides supervisory authority for competent authorities to collect reports, conduct on-site inspections, order for improvement and rescission of certification of incorporation, with penalties for refusal to report. Together with related laws such as the Act on Prevention of Transfer of Criminal Proceeds, these provisions constitute an institutional framework to address the risk.

In addition, in June 2025, the Cabinet Office updated and published the "Guidance on Measures to Prevent the Financing of Terrorism by corporations engaging in specified non-profit activities" and notified the competent authorities and CESNAs of the updated guidance. This guidance provides specific measures that CESNAs should take to prevent their activities from being misused for terrorist financing, contributing to mitigate the risk.

Furthermore, from October 2023, the monitoring based on a risk-based approach has been implemented, in which the competent authorities select target CESNAs based on the activities of CESNAs and areas of operation and approach CESNAs individually. This monitoring is a highly effective measure based on detailed implementation procedures, and is considered to contribute to further mitigating the TF risk for CESNAs.

(2) Public Interest Corporation <Jurisdiction: Cabinet Office>

(i) Characteristics

Public interest corporations, established for conducting public interest projects under the Act on Authorization of Public Interest Incorporated Associations and Public Interest Incorporated Foundations, encompassing activities in academia, arts, charity, and other fileds that contribute to the benefit of a broad and unspecified public.

To become a public interest corporation, a general incorporated association or foundation must apply for public interest certification, undergo deliberation and recommendation by a third-party organization (such as the Public Interest Certification Committee), and receive certification from the administrative agency.

As of September 1, 2025, there are 9,815 public-interest corporations (preliminary figure).

(ii) The vulnerabilities related to terrorist financing

The following points can be cited as structural vulnerabilities that could make public interest corporations susceptible to abuse for terrorist financing.

● Operating in regions exposed to the threat of terrorism or in conflict areas

A very small number of public interest corporations operate in regions where terrorist acts occur or their surroundings, and activities in these areas are considered to carry relatively higher risks compared to other regions.

● Engaging in outsourcing or grant assistance to carry out operations abroad

Public interest corporations may not only conduct activities directly but also operate through outsourcing or grant assistance to businesses or partner organizations abroad. In such cases, different entities handle the fundraising and disbursement of funds, making the use of funds less transparent and increasing the difficulty of fund management and verification of their use.

● Handling of substantial amounts of funds and use of cash abroad

Some public interest corporations receive substantial donations or grants and provide support through foreign remittances or the physical transfer of cash. Such cash transactions and transfers are highly anonymous, making it difficult to trace the flow of funds and increasing the risk of misuse.

(iii) Measures to Mitigate Risks

Public interest corporations are considered to have reduced the risk of terrorist financing to some extent by appropriate implementation of supervisory measures by the competent authority under the law, along with voluntary risk management efforts by each corporation. In particular, to prevent involvement in terrorist financing, it is important for each public interest corporation to have risk awareness based on the flow of its operations and to implement appropriate measures according to that risk. The "Countermeasures Against Terrorist Financing by

Public Benefit Corporations” published by The Cabinet Office in June 2022 provides examples of concrete measures tailored to the actual circumstances of corporations, encouraging proactive efforts by the corporations themselves. In addition, monitoring is conducted on selected target corporations based on a risk-based approach under certain standards.

As a result of these efforts, the risk of public interest corporations being misused for terrorist financing is considered to be mitigated to some extent.

(3) Social Welfare Corporation <Jurisdiction: Ministry of Health, Labour and Welfare>

(i) Characteristics

Social Welfare Corporations are legal entities established with the purpose of conducting social welfare activities under the Social Welfare Act (Act No. 45 of 1951). Social welfare activities are limited to those defined in the Social Welfare Act, including the operation of elderly care homes, child protection facilities, and the like. When establishing a social welfare corporation, the founding representative must prepare articles of incorporation, business plans, budget statements, and other required documents and obtain approval from the relevant authorities.

As of March 31, 2024, there are 21,118 social welfare corporations.

In addition, social welfare corporations are primarily established to carry out social welfare projects in Japan, such as those for the elderly and children, and their activities abroad are limited.

(ii) The vulnerabilities related to terrorist financing

The terrorist financing risk of social welfare corporations is analyzed based on the four evaluation perspectives indicated by the FATF: (a) products and services, (b) transaction types, (c) countries/regions, and (d) customer attributes.

● Products and services, and transaction types

Some social welfare corporations handle cash or remittances in relation to foreign support, but the frequency and scale of such transactions are limited.

● Countries/regions

Cases of activities abroad are limited, and no operations in high-risk areas such as conflict zones have been confirmed.

● Customer attributes

Most counterparties are entities equivalent to public institutions or businesses whose attributes have been verified.

Based on these factors, even for social welfare corporations engaged in activities abroad, the risk of terrorist financing is currently considered limited, and there are no significant vulnerabilities.

(iii) Measures to Mitigate Risks

When social welfare corporations conduct activities abroad, it is required to clearly state this in its articles of incorporation and obtain approval from the relevant authority. In addition, to distinguish domestic operations from activities abroad, it is mandatory to prepare financial statements separated by location. Furthermore, in the annual status report that must be submitted each year, if a social welfare corporation has conducted activities abroad, it is required to specify that such activities were carried out, along with details of the projects and the countries where they were implemented. Based on this information, the competent authority conducts appropriate monitoring. Through these mechanisms, the risk of terrorist financing in social welfare corporations is considered to be mitigated by certain institutional measures.

(4) Medical Corporation <Jurisdiction: Ministry of Health, Labour and Welfare>

(i) Characteristics

Medical corporations are legal entities established under the provisions of the Medical Care Act (Act No. 205 of 1948) and require approval from the governor of a prefecture to establish and operate hospitals, clinics, and similar facilities.

As of March 31, 2025, there are 59,419 medical corporations.

The activities of medical corporations abroad are limited to the operation of foreign medical institutions and the provision of medical technology and training to local healthcare professionals. These activities require approval from the relevant authorities. As of July 1, 2024, 10 medical corporations are engaged in activities abroad.

(ii) The vulnerabilities related to terrorist financing

Similar to social welfare corporations, the vulnerabilities of medical corporations related to terrorist financing risk were analyzed based on the four perspectives indicated by the FATF: (a) products and services, (b) transaction types, (c) countries/regions, and (d) customer attributes.

● Products and services

The services provided are limited to medical care and have little direct connection to supporting terrorist organizations.

● Transaction types

Some corporations have been confirmed to handle cash or engage in transactions with foreign entities, but the scale and frequency are limited.

● Countries/regions

Most activities are limited to domestic operations, and any foreign activities are restricted to medical support purposes.

● Customer attributes

Service recipients are mainly individuals such as patients and healthcare professionals, and the attributes of transaction counterparts are clearly identifiable.

Based on these factors, the inherent vulnerabilities of medical corporations are limited, and at present, the risk of their being misused for terrorist financing is considered relatively low.

(iii) Measures to Mitigate Risks

For medical corporations, in addition to the major statutory measures in Japan that contribute to reducing the risk of terrorist financing, institutional measures are taken through the general supervisory authorities under the Medical Care Act. Specifically, when medical corporations develop new businesses abroad, they are obligated to amend their articles of incorporation and obtain approval from the relevant authority for conducting activities overseas. Furthermore, when investing in foreign countries, they are required to submit a prior notification.If a medical corporation suspends its activities for a certain period, procedures for dissolution are provided under the system, and regular supervision by the competent authority is conducted based on the annual activity reports. Through these institutional measures, the risk of terrorist financing in medical corporations is considered to be reduced to a certain extent.

(5) School Corporation <Jurisdiction: Ministry of Education, Culture, Sports, Science and Technology>

(i) Characteristics

School corporations are legal entities established with the purpose of establishing and operating private schools. Their establishment is subject to approval by the relevant authority under the Private School Act (Act No. 270 of 1949), which stipulates the purpose, name, and other matters in the act of donation.

As of May 1, 2024 there are 7,848 school corporations.

School corporations are established with the purpose of establishing and operating private schools and their activities abroad are limited.

(ii) The vulnerabilities related to terrorist financing

Similar to social welfare corporations, the vulnerabilities of school corporations related to terrorist financing risk were analyzed based on the four perspectives indicated by the FATF: (1) products and services, (2) transaction types, (3) countries/regions, and (4) customer attributes.

● Products and services, and transaction types

Handling of cross-border transactions is permitted for some corporations, but the services provided are limited to educational activities, and monetary transactions are restricted to tuition fees, research-related expenses, and similar purposes.

- Countries/regions

The majority of overseas activities consist of educational and research activities or related projects, and as of the 2022 survey, 98% fell into this category.

- Customer attributes

Counterparties in cross-border transactions are limited to businesses certified by public authorities, students, or individuals whose attributes have been verified.

Based on this, the risk of terrorist financing in school corporations is considered limited, and no significant vulnerabilities are recognized at present.

(iii) Measures to Mitigate Risks

Regarding school corporations' activities, regardless of whether activities are conducted abroad, they are obligated to prepare financial documents, business reports, and related records every fiscal year and keep them at the office for inspection by interested parties. Furthermore, school corporations receiving subsidies from the relevant authorities are required to submit the copy of these documents to those authorities, and the authority conducts reviews and supervision of such content. Additionally, when engaging in activities aimed at generating revenue beyond educational and research activities, school corporations must specify this in their stipulated donation practices and obtain approval from the relevant authorities. Through these institutional frameworks, the risk of terrorist financing in school corporations is considered to be reduced to a certain extent.

(6) Religious Corporations <Jurisdiction: Ministry of Education, Culture, Sports, Science and Technology>

(i) Characteristics

A religious corporation is a corporation established under the Religious Corporations Act (Act No. 126 of 1951) for the purpose of enabling religious groups to obtain legal entity status. To establish such entities, they must obtain approval by the relevant authority for its rules, which must specify prescribed matters such as their objectives, name, and other required details.

As of December 31, 2023, there were 178,921 religious corporations in existence, with approximately 99% of them, or 177,753, falling under the jurisdiction of prefectural governors (the vast majority of which possess places of worship located solely within the area of a single prefecture). In addition, according to a sample survey, approximately 72% of all religious corporations, excluding comprehensive religious corporations, have annual operating revenues of less than 5 million yen[*1].

(ii) The vulnerabilities related to terrorist financing risks

Religious corporations have the following structural characteristics, which may constitute risk factors for misuse in terrorist financing and other illicit activities.

- Lack of transparency in actual activities

There is a certain number of religious corporations that were established as religious entities but are effectively inactive (hereafter referred to as "inactive religious corporations"). If such cases are left unattended, there is a risk that their legal status could be fraudulently used by third parties for purposes such as terrorist financing, tax evasion, or profit-oriented activities.

- Inadequate updating and reporting of corporate information

In some inactive corporations, cases have been identified where the whereabouts of the representative officer are unknown or financial documents have not been submitted for an extended period, making it difficult to ascertain the actual status of such corporations.

As of December 31, 2024, 5,019 corporations have been identified as inactive corporations.

[*1] Survey report on activities conducted by religious corporations (as of October 1, 2021).

(iii) Measures to Mitigate Risks

Religious corporations are obligated to create financial documents and other related materials annually. These documents are to be always kept in the office, and are subject to requests for inspection by believers and other stakeholders, as well as the requirement to submit copies to the relevant authorities.

The Agency for Cultural Affairs is strengthening efforts to ensure that all religious corporations properly fulfill their legal obligations, including rigorous enforcement of reminders and proper implementation of penalty measures, and enhanced measures to address inactive corporations. In March 2023, it issued a notice to prefectures and has since provided direct explanations through meetings of relevant department and division heads.

Specifically, prefectures are requested to take the following measures:

- Rigorous enforcement of reminders to corporations that have failed to submit copies of documents required to be kept at their offices.
- Proper implementation of penalty measures against corporations that are unlikely to submit the required documents.
- Clear specification of the criteria for determining inactive religious corporations (such as unknown whereabouts of the representative officer or consecutive failures to submit required documents)

In addition, through the Project for Promoting Measures against Inactive Religious Corporations, which began in fiscal year 2023, support is provided for initiatives undertaken by prefectures. Furthermore, through training sessions for prefectural officials in charge of religious corporation administration and other forums, attention is drawn to the risk of inactive religious corporations being misused by criminal organizations. Through these measures, the risk of terrorist financing in religious corporations is considered to be mitigated to some extent from an institutional perspective.

(7) Other Organizations

(i) Characteristics

Organizations that engage in "Good works" as defined by the FATF include general incorporated associations, general incorporated foundations, and voluntary organizations without juridical personality. These organizations are capable of conducting charitable activities and international cooperation activities, among others.

The Ministry of Foreign Affairs of Japan and Japan NGO Center for International Cooperation(JANIC)'s report[*1], revealed that 25 general incorporated associations and general incorporated foundations and 99 voluntary associations conduct activities as a "civil nonprofit organization conducting international cooperation."

The report also found that more than 80% of Japanese NGOs have no foreign offices, indicating that their activities outside of Japan are limited, and an analysis of the international NGO database revealed that 75% of registered voluntary organizations have an organization size (revenue size) of less than 10 million yen, and the largest does not exceed 40 million yen, indicating that overall organizational size tends to be small.

(ii) Measures to Mitigate Risks

Among general incorporated associations, general incorporated foundations, and voluntary organizations that meet the FATF definition of nonprofit organizations but are not subject to certification, accreditation, or registration because of their legal status, such organizations are usually small and have a limited area of activities. In principle, fund transfers are conducted through financial institutions.

Furthermore, general incorporated associations and general incorporated foundations, which are not subject to certification, accreditation or registration, are generally larger than voluntary organizations but are obliged to register as a legal person under the Act on General Incorporated Associations and General Incorporated Foundations (Act No.48 of 2006). Violations of this obligation are subject to penalties (fines), and investigating authorities have access to the registered information on those legal persons and deterrent and tracing measures commensurate with the risk

[*1] Ministry of Foreign Affairs and Japan NGO Center for International Cooperation, "NGO Databook 2021: Statistics on Japan's NGOs" (February 2022)

are in place. Through these institutional frameworks, a certain level of monitoring and regulatory environment is ensured even for these corporations. Therefore, the risk of these entities being misused for TF is relatively low compared to nonprofit legal entities under the six aforementioned laws.

3. Assessment of Risks

In Japan, nonprofit organizations with the following characteristics are considered to have a relatively higher risk of being misused for terrorist financing.

- Nonprofit organizations operating in regions where terrorist activities are being carried out or in their vicinity.
- Nonprofit organizations handling significant amounts of funds and conducting international fund transfers or cash transactions abroad.
- Nonprofit organizations with unclear legal entities, such as those in a dormant state.

Regarding financial transactions involving these organizations, it is necessary to take into account observations from international bodies, given Japan's role in the international financial market.

It should be noted that there have been no cases of nonprofit organizations being prosecuted for being exploited for terrorist financing in Japan and the proportion of nonprofit organizations conducting activities abroad is also limited. Taking these factors comprehensively, it is considered that they are at a low risk of abuse at present.

However, taking into account the increasing international concerns about the misuse of nonprofit organizations for terrorist financing in recent years, it remains important in Japan to continuously review the risk assessment of nonprofit organizations. Competent authorities are expected to conduct monitoring according to the risk. In addition, for nonprofit organizations operating in high-risk regions, it is considered important to continuously carry out outreach regarding the risks of terrorist financing and the measures to combat them, to ensure the soundness of their activities.