November 2024

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

The situation surrounding money laundering and terrorist financing (hereinafter referred to as "ML/TF") in Japan is changing rapidly, and the measures required internationally are also evolving. In responding to such changes and international requirements, it is important for stakeholders in Japan to fully understand the risks and to implement measures that are tailored to those risks as we strengthen our AML/CFT (Anti-Money Laundering and Countering the Financing of Terrorism) measures.

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, jointly chaired by the National Police Agency and the Ministry of Finance. This was done to enforce the Government's AML/CFT/CPF measures as a whole. At the same time, the Government of Japan formulated an AML/CFT/CPF action plan for the next three years.

The Inter-Ministerial Council aims to plan and formulate national policies and activities related to AML/CFT/CPF measures, while also ensuring close cooperation among relevant ministries and agencies. In May 2022, the Inter-Ministerial Council formulated the "Strategic Policy towards Promoting AML/CFT/CPF" (hereinafter referred to as the "Strategic Policy") in order to examine the risks surrounding Japan and purposes of AML/CFT/CPF measures of Japan, and improve the effectiveness of the measures. The Strategic Policy states that the Government will take effective AML/CFT/CPF measures based on the contents of the National Risk Assessment-Follow-up Report (hereinafter referred to as the "NRA-FUR"), which reflects the current state of risks in Japan. It outlines 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.

Through a united effort of the government and the private sector based on the Action Plan and the Strategic Policy, AML/CFT measures are steadily progressing in Japan. However, due to the rapid changes in new technological advancements and domestic and international criminal environment, the measures commensurate with the risks are also constantly changing.

The Inter-Ministerial Council, looking ahead to the Fifth Round of Mutual Evaluation of Japan by the FATF (Financial Action Task Force), formulated a new "National AML/CFT/CPF Action Plan (FY2024-26)" in April 2024 to enhance the effectiveness of AML/CFT measures and to respond to changes in risks.

Based on these Strategic Policy and Action Plans, by promoting further information sharing among relevant ministries and agencies through the framework of the Inter-Ministerial Council, as well as collaboration between the public and private sectors, the NRA-FUR is updated timely and appropriately regarding the risks of ML/TF in Japan. This ensures that the premise for a risk-based approach is provided.

This NRA-FUR aims to promote understanding of the risks of ML/TF in Japan, to assist in AML/CFT measures commensurate with the risks, and ultimately to prevent the transfer of criminal proceeds, ensuring the safety and peace of citizens' lives and contributing to the sound development of economic activities.

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 Inter-Ministerial Council published the "National Risk Assessment of Proliferation Financing in Japan" in March 2024. 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], 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 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[*3]. 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[*4] 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 understood as shown in the following table. It is based on the "National

---

*1 Article 8, paragraph (3) of the Act on Prevention of Transfer of Criminal Proceeds, "Suspicious transaction report (STR), etc."

*2 Article 11, paragraph (1), item (iv) of the Act on Prevention of Transfer of Criminal Proceeds, "Measures to properly conduct verification at the time of transaction, etc."

*3 Financial Service Agency "'Anti-Money Laundering, Counter Financing of Terrorism, and Counter-Proliferation Financing' Current Status and Challenges (June 2024)"; National Police Agency "Annual Report," "The White Paper on Police," "Situation of organized crime"; Ministry of Justice "White Paper on Crime," etc.

*4 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.

Money Laundering 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: Boryokudan, Anonymous and fluid criminal groups, and Crime groups of foreigners in Japan Predicate offences: Theft, fraud, 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[*3] 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 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, and the private sector for AML/CFT measures, 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
- ○ 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 JAFIC.

4. Overview of NRA-FUR

(1) Overview of This Year's NRA-FUR

Section 2 of this NRA-FUR describes the "environment surrounding Japan," which is the premise for a comprehensive view of the various ML/TF-related risks surrounding Japan, in terms of geographical, social, economic, and criminal environments. Section 3 analyzes the offenders of ML/TF, such as Boryokudan, Anonymous and fluid criminal groups and Crime groups of foreigners in Japan, which are perceived as threats to Japan, the main predicate offences such as theft, fraud and drug-related offences, and the modus operandi such as main methods of transactions, misused for ML/TF.

Next, Section 4 describes high-risk transactions. Transactions that are evaluated as high-risk are, from the perspective of "transaction types," non-face-to-face transactions, cash transactions, and cross-border transactions; from the perspective of "countries/regions," transactions that have ties to Iran or North Korea and transactions with countries/regions for which the FATF statement requires the application of enhanced customer due diligence commensurate with the risk; and from the perspective of "customer attributes," transactions with Boryokudan, international terrorists, and non-resident customers for whom customer due diligence is difficult, foreign politically exposed persons (Foreign PEPs), and legal persons without transparency of beneficial owners.

Furthermore, Section 5 evaluates risk from the perspective of "products and services." It assesses that the products and services handled by specified business operators, such as deposit-taking institutions, funds transfer service

providers, and cryptoassets exchange service providers, are relatively riskier than those of other business types. It also evaluates that services handled by electronic payment instruments service providers are expected to be relatively of high-risk. Lastly, Section 6 shows low-risk transactions for which simplified CDD is allowed.

[Overview of NRA-FUR]

<table>
<tr><td colspan="5">Section 1. Risk Assessment Method.</td></tr>
<tr><td colspan="5">Section 2. Environment Surrounding Japan</td></tr>
<tr><td colspan="5">Geographic environment, social environment, economic environment, criminal environment</td></tr>
<tr><td colspan="5">Section 3. Analysis of Money Laundering Cases</td></tr>
<tr><td>1.Offenders</td><td colspan="4">Boryokudan, Anonymous and fluid criminal groups, and Crime groups of foreigners in Japan</td></tr>
<tr><td rowspan="2">2.Modus Operandi</td><td colspan="4">Predicate offences (thefts, frauds, etc.)</td></tr>
<tr><td colspan="4">Major transactions misused for money laundering</td></tr>
<tr><td colspan="5">3.Suspicious Transaction Report (STR)</td></tr>
<tr><td colspan="5">Section 4. High-risk Transactions</td></tr>
<tr><td>1.Transaction Types</td><td colspan="4">Non-face-to-face transactions, cash transactions, cross-border transactions</td></tr>
<tr><td>2.Countries/Regions</td><td>Particularly high</td><td>Iran and North Korea</td><td>High</td><td>Myanmar</td></tr>
<tr><td rowspan="2">3.Customer Attributes</td><td>Persons who intend to commit ML/TF</td><td colspan="3">"Boryokudans"
International terrorists</td></tr>
<tr><td>Persons for whom it is difficult to conduct CDD</td><td colspan="3">Non-residents, foreign PEPs, legal persons (legal persons without transparency of beneficial owners)</td></tr>
<tr><td colspan="5">Section 5. Risk of Products and Services</td></tr>
<tr><td>Relatively higher risk than other business forms</td><td colspan="4">Products and services dealt with by deposit-taking financial institutions
Funds transfer services, cryptoassets
Electronic payment instruments (expected to have a relatively higher risk)</td></tr>
<tr><td>Considered to be of risk</td><td colspan="4">Insurance, investment, trust, money lending, foreign currency exchanges, financial leasing, credit cards, real estate, precious metals and stones, postal receiving services, telephone receiving services, telephone forwarding services, legal/accounting services</td></tr>
<tr><td colspan="2">Products and services using new technologies that should be monitored closely</td><td colspan="3">High-value electronically transferable prepaid payment instruments
Casinos</td></tr>
<tr><td colspan="5">Section 6. Low-risk Transactions</td></tr>
<tr><td>Factors that Mitigate Risks</td><td colspan="4">Source of funds is identified, the customer, etc., is the national government or a local public entity, the customers, etc., are limited under laws and regulations, the transaction process is supervised by the national government, etc. based on laws, etc., it is difficult to disguise the actual status of legal persons, etc., minimal or no fund-accumulation features, the transaction amount is less than the regulatory threshold, customer identification measures are secured by laws, etc.</td></tr>
<tr><td colspan="5">Types of Low-risk Transactions</td></tr>
</table>

(2) 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	○Added analysis of factors that increase risk in the "precious metals and stones" category of products and services in which risk is recognized ○Added analysis of factors that increase risk in the category of high-risk cross-border transactions ○Excluded "transactions with customers who use non-photo identification" from the list of high-risk transactions
December 2018	○Added analysis of threats such as virtual currency and gold smuggling, international ML, and ML using legal persons, as well as analysis of vulnerabilities in the management systems of telephone forwarding service providers ○Added descriptions of specific examples of efforts by business operators and modus operandi of ML cases in order to promote AML/CFT ○Added descriptions regarding casinos
December 2019	○Added information on risks and countermeasures in light of the increase in the number of foreigners ○Added examples of cases in which arrests were made as a result of STRs in order to promote efforts to submit STRs
November 2020	○Added descriptions regarding environment surrounding Japan ○Expanded descriptions of 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 where legal persons without transparency, funds transfer services, and cryptoassets were misused for ML, as well as information regarding STRs ○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

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

The 2024 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) Among the offenders in ML (Boryokudan, online and telephone fraud group, and Crime groups of foreigners in Japan), "online and telephone fraud group" have been changed to " Anonymous and fluid criminal groups," and descriptions have been added of fundraising activities such as investment / romance fraud via social media, which are seeing a sharp increase in cases.

(ii) In light of the fact that shell companies or opaque companies and corporate accounts are being misused for ML, the analysis of legal persons (legal persons without transparency of beneficial owners, etc.) has been deepened.

(iii) International situations and cases, including those in neighboring countries, are introduced from reports on cyber-related fraud (CEF) by the FATF, the Egmont Group, and the ICPO, as well as from the APG's typology report. As advances in digital technology are expected to increase the threat of cross-border ML/TF, situations and cases from other countries have similarities with Japan, and are useful as reference for potential threats.

(iv) Topics related to consideration of revisions to the FATF Recommendations for high-risk cross-border transactions have been added, and topics related to international trends for high-risk cryptoassets have been updated.

(v) Examples have been added of STRs of high-risk non-face-to-face transactions, cash transactions, and cross-border transactions. In addition, the method of describing examples of STR utilization has been reviewed and updated.

(vi) As part of investigation of the operational aspects of risk mitigation measures for specified business operators, items that the competent authorities have identified and that business operators should be aware of are described.

(vii) Since the volume of the NRA-FUR increased due to the deepening of analysis and the addition of recent specified business operators as described above, the table of contents was subdivided and a bookmark function was added, charts were utilized, supplementary explanations were added regarding the positioning of each item, and items such as the risk assessment method were updated in order to facilitate user understanding.

[Comprehensive Measures to Protect People from Fraud]

In recent years, as social media and cashless payments have become more widespread, modus operandi of fraud and other crimes that misuse science and technology have rapidly become more sophisticated and diverse, and the damage caused by such frauds is expanding at an accelerating rate.

In light of this situation, Comprehensive Measures to Protect People from Frauds was decided at the Ministerial Conference on Measures against Crime on June 18, 2024, in order to keep up with the speed of change and take even stronger measures via public-private partnership to protect people from damages caused by frauds.

The comprehensive measures are designed to evolve and replace 'Plan to Combat "It's Me" Fraud' (adopted at the Ministerial Conference on Measures against Crime on June 25,2019) as well as plan for emergency measures against robbery and special fraud cases involving the recruitment of perpetrators on social media (adopted at the Ministerial Conference on Measures against Crime on March 17,2023) and consolidate comprehensive measures targeting communications fraud, investment/romance fraud via social media, and phishing. The government aims to work together to promote these measures in cooperation with related agencies and organizations.

The main initiatives of the comprehensive measures are as follows[*1]:

1. Measures to "prevent people from becoming victims"

Investment/romance fraud via social media

- Effective publicity and awareness-raising according to the situation of damage occurrence, etc.
- Promotion of effective examination of advertisements by social media service providers, etc.
- Promotion of appropriate responses such as removal of spoofing-type false advertisements
- Mandating large-scale platform operators to take measures to speed up the response to removals and make their operational status transparent
- Implementation of effective warning displays and consent acquisition when adding unknown accounts as friends
- Strengthening identity verification when opening official social media accounts and matching app accounts
- Raising awareness of damage prevention in the newly started financial education

Anti-phishing measures

- Promotion of response to sender domain authentication technologies (DMARC, etc.)
- Promotion of closure of phishing sites
- Preemptive measures based on the characteristics of phishing sites

Measures against communications fraud

- Expansion of the system for accepting applications for suspension of international phone calls
- Promotion of measures against inappropriate use of SMS
- Promotion of measures to warn people who use ATMs while using mobile phones

2. Measures to prevent people from getting involved in crime

- Promotion of collection, removal, and control of information on so-called "Yami Baito" (shady part time job), etc.
- Education and awareness-raising to prevent young people from being involved in crimes as if it were a part-time job

3. Measures to deprive criminals of tools

- Efforts to ensure the effectiveness of identity verification
- Promotion of arrest measures in cooperation with financial institutions
- Measures to prevent the use of electronic money in crimes
- Strengthening measures to prevent the illicit use of deposit/savings accounts, etc.
- Promotion of confiscation and preservation of cryptoassets

4. Measures to prevent criminals from escaping

- Strengthening the system for control and clarification of Anonymous and fluid criminal groups
- Requesting social media providers to strengthen their response to inquiries from law enforcement agencies
- Promotion of the detection of overseas criminal bases, etc.
- Promotion of efforts to prevent legal persons from being misused for ML
- Promotion of recovery of property damage

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

Section 2. Environment Surrounding Japan

This section describes the geographic, social, economic and criminal environments that constitute the premise of ML/TF threats in Japan.

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, 2023, was approximately 124.35 million, marking 13 consecutive years of decrease. The ratio of the population aged 65 and over to the total population reached a record high of 29.1%, which is higher than in other developed countries. In Japan, the population is aging rapidly while also decreasing. In the future, it is estimated that the total population of Japan will steadily decline to less than 100 million in 2056.

The number of foreigners entering Japan*[1] in 2023 was approximately 25.83 million. This represents a significant increase from the previous year's 4.2 million, and has recovered to 82.8% of the level in 2019, before the COVID-19 pandemic. The total number of new entrants was approximately 23.75 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 Hong Kong. Regarding the purpose of entry (status of residence), the number of Temporary Visitors was the largest at approximately 23.13 million (97.4%), followed by foreigners with the residence statuses of Technical Intern Training at approximately 180,000 (0.8%), and Student at approximately 140,000 (0.6%), respectively.

The number of foreign residents as of the end of 2023 was approximately 3.41 million, 10.9% more than the previous year. In terms of the number of foreign residents by nationality and region, China*[2] was the largest and accounted for 24.1% of the total, followed by Vietnam, South Korea, the Philippines, and Brazil.

3. Economic environment

The Japanese economy occupies a vital position in the world economy. The nominal GDP in 2023 (Quarterly Estimates of GDP for Apr.-Jun. 2024 (The Second Preliminary Estimates)) was 592.8 trillion yen, the fourth-largest economy after the United States, China, and Germany. The real GDP growth rate in FY2023 was 0.8%. The share of nominal gross value added by economic activity (industry) in 2022 was 1.0% for the primary industry, 24.7% for the secondary industry, and 74.3% for the tertiary industry. Regarding the trade value in 2023, Japan’s exports amounted to 100.8738 trillion yen, and imports amounted to 110.1956 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, Taiwan.

---

*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."

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

The annual number of notifications*[1] of STRs related to the main countries subject to economic sanctions between 2021 and 2023 is as shown in Table 1.

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 is nationwide, and funds can be transferred quickly and reliably. As of the end of March 2023, the number of branch offices of major financial institutions*[2] was 37,293 (including 172 branch offices located abroad). There were 85,000 ATMs*[3] 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 2023 were Japanese financial institutions.

In terms of the scale of financial transactions in Japan, the balance of bank deposits at the end of March 2024 was approximately 1,180 trillion yen. As for settlement transactions in 2023, domestic exchange transactions comprised approximately 3,535 trillion yen (approximately 2 billion cases), with a daily average of about 14 trillion yen (approximately 8.05 million cases), and the amount of foreign exchange in settled in yen was approximately 5,455 trillion yen (approximately 7.84 million cases), with a daily average of about 22 trillion yen (approximately 32,000 cases).

Looking at the size of the securities market, as of the end of December 2023, the total market capitalization of stocks in Japan was approximately 867 trillion yen. During 2023, the trading value of listed stocks on the Tokyo Stock Exchange was about 944 trillion yen in the Prime Market, 30 trillion yen in the Standard Market, and 38 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, with the rise in the ratio of cashless payments*[4] due to the promotion of cashless transactions, the proportion of cash usage in payments has relatively decreased. The advancement of cashless transactions is expected to contribute to the suppression of ML/TF related to cash transactions.

---

*1 The annual number of notifications refers to the number of STRs notified to the National Public Safety Commission and the National Police Agency by the competent authorities.

*2 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.

*3 The total number of city bank, regional bank, trust bank and second regional bank ATMs was calculated as of the end of September 2023, and the number of Japan Post Bank ATMs was calculated as of the end of March 2023.
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.

*4 According to the calculations by the Ministry of Economy, Trade, and Industry, the cashless payment ratio in 2023 increased from 26.8% in 2019 to 39.3%.

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 do ML/TF. Once criminal proceeds are invested in Japan's economic activities through Japan's financial system and are mixed in with vast amounts of legal funds and transactions, it will be exceedingly difficult to identify and track criminal proceeds from among them.

Table 1: Annual Number of Notifications of STRs Related to Main Countries under Economic Sanctions

Destination (Origin) Country or Jurisdiction	2021	2022	2023
Iraq	9	8	26
Democratic Republic of the Congo	58	70	110
Sudan	4	3	6
North Korea	1	1	1
Somalia	1	1	2
Libya	0	0	1
Syria	2	1	1
Russia	901	917	774
Belarus	21	14	14
Central African Republic	1	0	0
Yemen	4	3	3
South Sudan	0	0	0
Mali	5	2	4
Haiti	3	1	3

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 has consistently decreased from 2003 to 2021. However, in 2023, there were 703,351 cases, increasing for the second consecutive year compared to the post-war record low in 2021 (an increase of 17.0% from the previous year). The flow of people in each region is returning to the level before the COVID-19 pandemic, and the number of recognized criminal offence cases is approaching the level of 2019, indicating a situation that requires close attention for future trends.

Among these, the trend in the amount of damage from offences against property* [1] has increased by 56.7% from the previous year to approximately 251.9 billion yen. Looking at the breakdown of this figure, the amount of damage caused by fraud increased to 162.6 billion yen (an increase of 85.4% from the previous year). Furthermore, it was observed that the increase in damage caused by fraud was due in part to an increase in frauds using the Internet.

* [1] Armed robbery, extortion, theft, fraud, embezzlement, and embezzlement of lost property

(ii) Cyber Crimes[*1]

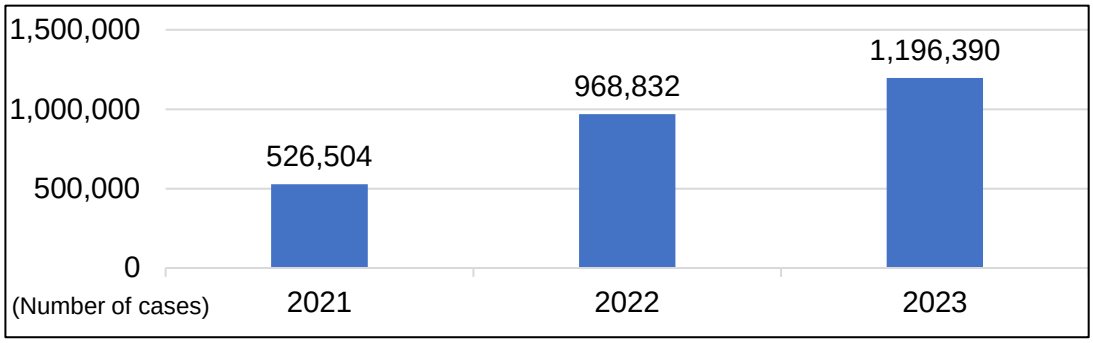
The threat situation surrounding cyberspace in 2023 remains extremely serious, with the following situations observed:

- ○ The amount of damage caused by credit card fraud in 2023 was the highest ever (54.09 billion yen).
- ○ The amount of damage caused by online banking fraud in 2023 was the highest ever in both the number of cases and amount of damage (5,578 cases, approximately 8.73 billion yen).
- ○ The number of reported cases of ransomware damage in 2023 remained high at 197 cases, and 30 cases of damage from "no-ware ransom," that is, encryption-less ransomware, where offenders steal data without encrypting it and then demand payment, were confirmed.
- ○ There were numerous cases of unauthorized access to administrative agencies, academic research institutions, etc., that were suspected to be attempts to steal information.

(A) Situation of Phishing

According to the Council of Anti-Phishing Japan, the number of reported phishing cases in 2023 was 1,196,390 (an increase of 227,558 from the previous year), the highest number ever. Most of the phishing attacks were from offenders impersonating credit card operators and e-commerce business operators.

Table 2: Trends in the Number of Reports on Phishing



[*1] 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.

[Topic] Clarification of the Actual Status of Chinese Phishing Groups

Phishing victims have been reported all over the world, and many cases have been confirmed in Japan as well. In some cases, offenders have stored millions of IDs, passwords, and tens of thousands of pieces of credit card information on their own devices.

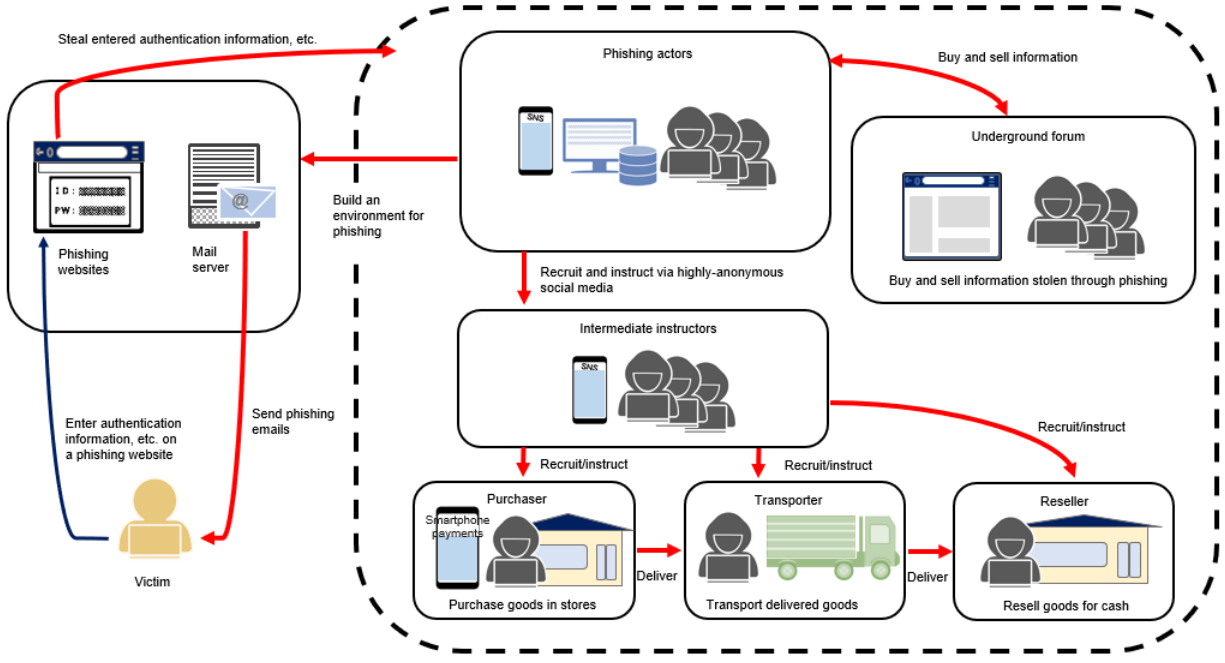
In addition, investigations into phishing cases in Japan and cases of the unauthorized use of information leaked through phishing have revealed the existence of a Chinese group that conducts phishing in an organized manner.

The group has built an ecosystem that facilitates phishing. Specifically, it has been confirmed that the group recruits people who play intermediate instructional roles (hereinafter referred to as "intermediate instructors") and people who purchase products, etc., through highly anonymous social media, etc., and uses these social media, etc., as a means of communication. It was also confirmed that after the phishing actors steal IDs and passwords through phishing, the intermediate instructors instruct members to make unauthorized purchases of products by misusing smartphone payment services and credit card information, transport the purchased products, or resell them for cash, thereby obtaining unauthorized profits.

In addition, phishing actors are also considered to be buying and selling information stolen through phishing and providing phishing instructions through highly anonymous social media, etc.

Similar ecosystems are believed to have been built in other phishing cases as well, and efforts are continuing to investigate phishing cases and clarify the actual situation.

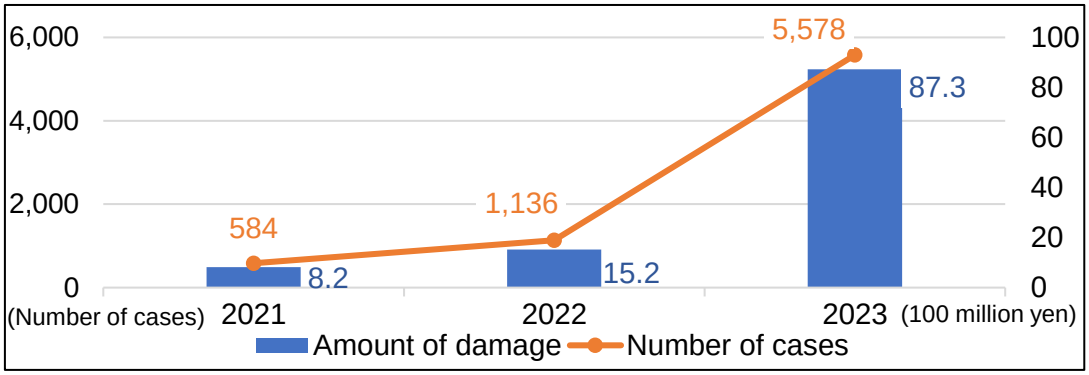
Table 3: Ecosystem that Facilitates Phishing Built by Chinese Phishing Group



(B) Situation of Online Banking Fraud Cases

In 2023, the number of online banking fraud cases was 5,578, and the amount of damage was approximately 8.73 billion yen, both of which are the highest ever.

Table 4: Trends in the Number of Online Banking Fraud Cases



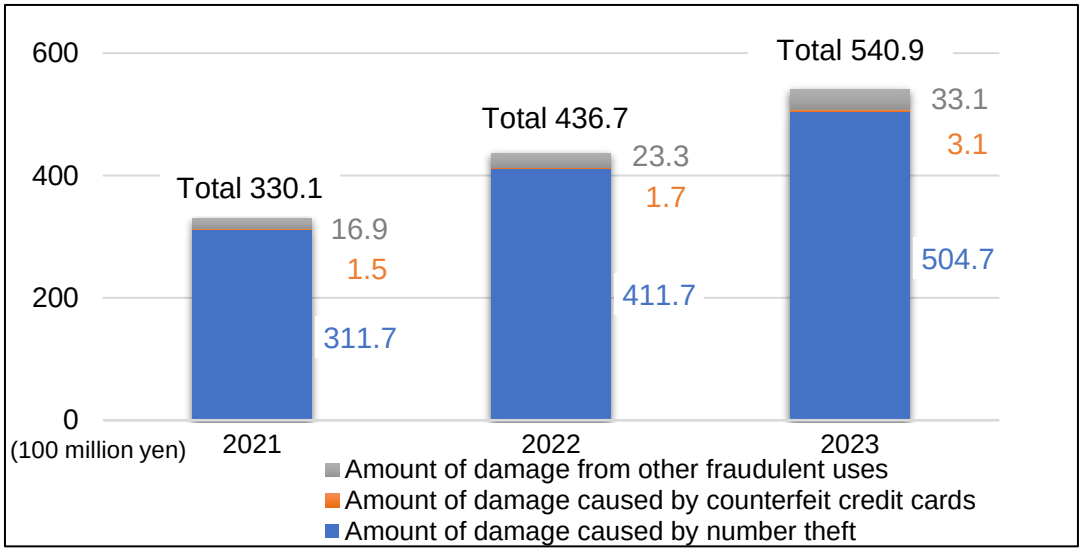
The characteristics of online banking fraud cases include the following:

- ○ The majority of victims are individuals, and by age, approximately 60% of victims are in their 40s to 60s.
- ○ The breakdown of modus operandi, 53% were via email and 21% were via SMS.
- ○ More than 50% of the fraudulent remittance amounts were fraudulently transferred to financial institution accounts of cryptoassets exchange service providers.

(C) Situation of Credit Card Fraud

The amount of damage caused by credit card fraud has been on the rise since 2013, with the amount of damage in 2023 reaching 54.09 billion yen, the worst since statistics began being collected in 1997* [1].

Table 5: Status of Credit Card Fraud Damage

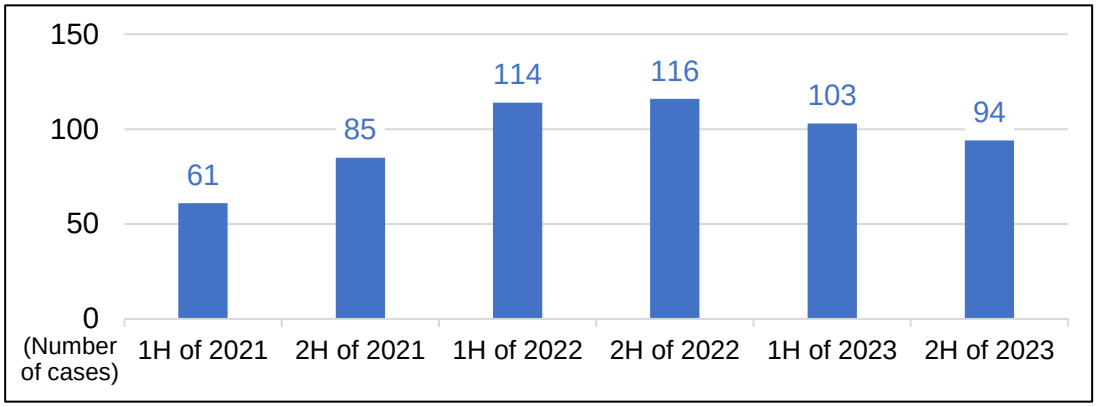


* [1] According to a survey by the Japan Consumer Credit Association.

(D) Situation of Ransomware

In 2023, the number of ransomware attack cases reported to the National Police Agency was 197, remaining at a high level.

Table 6: Trends in the Number of Reports on Ransomware Damage



Key characteristics of victims of ransomware attacks include the following:

- ○ Many of them were victims of double extortion[*1].
- ○ In many cases, criminals demanded payment in cryptoassets.
- ○ Regardless of size and industries, companies and organizations have become victims of ransomware attacks.

In addition to damage caused by ransomware, 30 cases[*2] of damage 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, were confirmed.

*1 "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."

*2 The number of cases of "no-ware ransom" is not included in the number of reports on ransomware damage in 2023 (197 cases).

[Topic] ML/TF related to Ransomware

1. About the FATF Report[*1]

FATF, in its report published in March 2023, highlights the following regarding the characteristics of ML/TF related to ransomware:

- ○ Most ransom payments and subsequent ML related to ransomware occur through cryptoassets, with cryptoassets exchanges being commonly used.
- ○ Ransomware attackers leverage the international nature of cryptoassets to conduct large-scale and near-instantaneous cross-border transactions. At times, transactions are carried out without the involvement of financial institutions that implement AML/CFT measures.
- ○ To further complicate transactions, ransomware attackers use highly anonymous cryptoassets, mixers, and other technologies/methods or tokens that enhance anonymity in ML.
- ○ Ransomware attackers often use non-hosted wallets like Unhosted Wallets*[2] and cryptoassets wallets of cryptoassets exchange service providers located outside the region where the attack occurred, and these operators do not collaborate with law enforcement agencies. Additionally, they use different addresses for each attack.
- ○ Many ransomware networks are connected to countries or regions with a high risk of ML, and they deposit or cash out their earnings in such countries or regions.

2. Key Focus Points When Submitting STRs

The risk indicators related to customers or transactions in ransomware, as outlined by the FATF, are as follows:

Indicators related to Ransomware Victims' Payments

- ○ Outgoing transfers to cybersecurity consulting companies or incident response companies handling ransomware recovery
- ○ Crypto-asset purchases on behalf of third parties by these companies
- ○ Unusual transfers from insurance companies specializing in ransomware recovery
- ○ Reports from customers regarding ransomware attacks or payments
- ○ Media coverage and reports related to ransomware attacks on customers
- ○ Large transactions from the same bank account to multiple accounts of crypto-assets exchange service providers
- ○ Payment details containing terms like "ransom" or the name of a ransomware group
- ○ Payments to crypto-assets exchange service providers located in high ML/TF (Money Laundering/Terrorist Financing) risk countries or regions
- ○ Transactions from customers with no crypto-asset trading history deviating from standard business practices
- ○ Transfers to third parties after customers have raised transfer limits
- ○ Transactions where customers express anxiety or urgency about payment timing
- ○ Purchases of privacy-enhanced crypto-assets
- ○ New customers buy crypto-assets and send account balances to a single address

Indicators related to Ransomware Attackers

- ○ Little or no activity in transactions after the initial large crypto-asset transfer
- ○ Identification of connections to ransomware through blockchain analysis
- ○ Immediate withdrawals after the return of crypto-asset funds
- ○ Sending crypto assets to wallets associated with ransomware
- ○ Utilization of crypto-assets exchange service providers in high ML/TF risk countries or regions
- ○ Sending crypto assets to mixing services
- ○ Use of encrypted networks
- ○ Mention of owning highly private email accounts in customer information
- ○ Inconsistencies in authentication information or requests for account opening with false identity information
- ○ Multiple accounts linked to the same contact with different names
- ○ Transactions related to privacy-enhanced crypto-assets

*1 Countering Ransomware Financing (March 2023)

*2 Refers to cryptoassets wallets managed by users themselves, not through cryptoassets exchanges or service providers.

(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 August 2021, the Taliban seized control of Kabul, the capital of Afghanistan, raising concern that Islamic extremist organizations may become increasingly active, utilizing Afghanistan as their base.

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 attacks against Israel and Western interests, and terrorist incidents believed to be related to this situation have occurred in various countries.

Furthermore, terrorist incidents are occurring around the world, and there have been actual cases in the past where Japanese nationals and Japan's national interest have been targeted by terrorist attacks. As such, it can be said that the threat of terrorism against Japan persists, and there are ongoing concerns that Japanese nationals may become victims of terrorism and kidnaping. Although many years have passed since the abductions perpetrated 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.

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 also describes the usage status of STRs in investigations.

The number of cleared ML cases[*1] in 2023 was 909, an increase of 183 cases compared to the previous year (see Table 7).

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, Table 8 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 2021 to 2023.

Table 7: Number of Cleared ML Cases

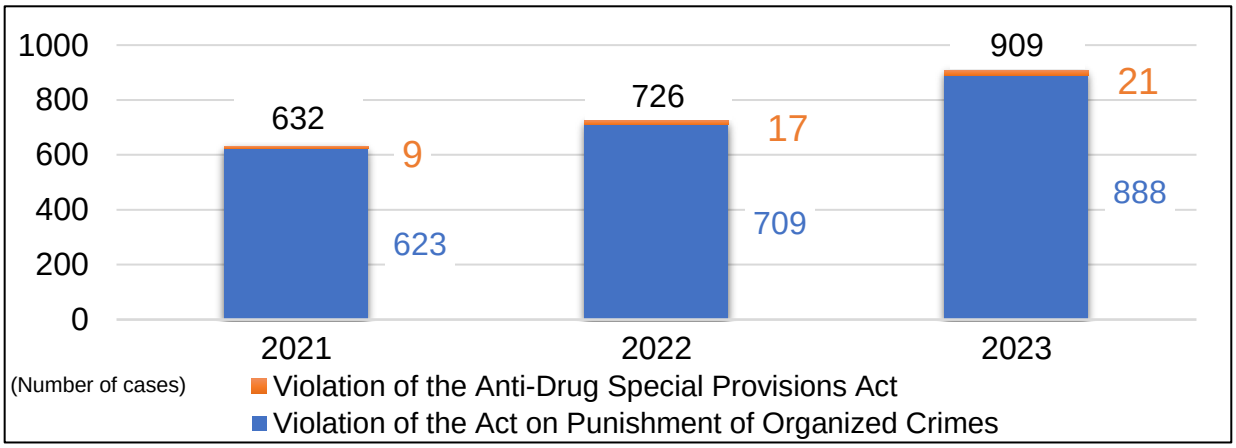


Table 8: Status of Confiscation of Criminal Proceeds

			2021	2022	2023
Preservation for confiscation before prosecution					
	Act on Punishment of Organized Crimes	Number of cases	142	162	211
		Total amount of money and claims (thousand yen)	507,211	1,047,244	1,044,378
	Anti-Drug Special Provisions Act	Number of cases	24	23	20
		Total amount of money and claims (thousand yen)	32,712	25,363	45,427
Confiscation					
	Act on Punishment of Organized Crimes	Number of persons	72	76	119
		Amount (thousand yen)	217,888	205,665	353,107
	Anti-Drug Special Provisions Act	Number of persons	51	56	54
		Amount (thousand yen)	10,465	5,678	8,404
Collection of a sum of equivalent value					
	Act on Punishment of Organized Crimes	Number of persons	62	92	103
		Amount (thousand yen)	1,476,380	1,342,766	1,267,096

*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.

	Anti-Drug Special Provisions Act	Number of persons	226	223	199
		Amount (thousand yen)	854,361	860,989	394,524

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 2024.
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 are "Boryokudan," "Anonymous and fluid criminal groups," 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) Boryokudan

In Japan, ML by Boryokudan remains a serious threat. Among cleared ML cases in 2023, 57 cases (6.3%) were related to Boryokudan members, associates, and other related parties (hereinafter referred to as "Boryokudan gangsters").

Table 9: Number of Cleared ML Cases Committed by Boryokudan Gangsters

Category \ Year	2021		2022		2023	
	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	10.1	64	8.8	57	6.3
Related to the Act on Punishment of Organized Crimes	60	9.6	62	8.7	54	6.1
Related to the Anti-Drug Special Provisions Act	4	44.4	2	11.8	3	14.3

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

The characteristics of fundraising activities 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 2023 it was a high 13.9%, indicating that fundraising 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.
- ○ Fundraising activities are conducted in a wide variety of areas, including finance, construction, labor dispatch, and adult entertainment businesses.

In addition, an analysis of status of cleared ML cases committed by Boryokudan gangsters from 2021 to 2023 revealed the following:

- ○ By predicate offences, fraud, computer fraud, and theft were common.
- ○ Regarding criminal proceeds, the total amount (limited to those that can be monetized) was approximately 1.39

billion yen. As to the form, cash including bank deposits accounted for 77.3% of the cleared cases, with an average of about 7.5 million yen per case.

- ○ When analyzed by transaction type, domestic exchange transactions[*1] accounted for 42.5% of all cases, while 21.2% of cases involved receiving cash without involving any goods or services.
- ○ Looking at the accounts used by Boryokudan gangsters, 84.0% were accounts under the names of fictitious or other parties, among which 23.4% were in the name of acquaintances of Boryokudan gangsters and 22.3% were in the name of family members, indicating that nearly half of the accounts used were in the names of those closely related to Boryokudan gangsters.

Furthermore, ML by Boryokudan seems to be carried out internationally. In July 2011, the United States published the "Strategy to Combat Transnational Organized Crime" and, in a Presidential executive order[*2] imposing economic sanctions, designated Japan's Boryokudan gangsters as one of the most serious transnational organized crime groups, and decided to freeze Boryokudan-related assets existing in the U.S. or possessed or managed by U.S. citizens. The U.S. also banned its citizens from dealing with Boryokudan gangsters.

(2) Anonymous and fluid criminal groups

To date, online and telephone fraud groups have been identified as ML offenders based on the number of cases recognized and the amount of damage, and have been analyzed in depth.

However, in 2023, the amount of damage from investment /romance fraud via social media exceeded that from online and telephone fraud, and changes in the criminal environment have been observed. Therefore, the scope of offenders has been expanded to include "Anonymous and fluid criminal groups" as offenders that engage in a wider range of fundraising activities, not limited to online and telephone fraud.

(i) Actual Situation

(A) Background

As the power of Boryokudan has been declining, there have been cases where people with bad behavior, including former members of Boryokudan and former members of motorcycle gangs, have committed crimes of assault and injury collectively and habitually in entertainment districts and amusement areas, without belonging to any specific organization such as Boryokudan. Although these groups do not have a clear organizational structure like Boryokudan, some are made up of loose ties based on human relationships such as senior and junior members, friends and acquaintances, and appear to have close ties with Boryokudan. The police have traditionally classified them as "quasi-Boryokudan," which are similar to Boryokudan, and have made efforts to strengthen control of these groups.

In recent years, in addition to quasi-Boryokudan, criminal groups with new characteristics have emerged, posing a threat to public security measures. In light of this situation, the police have positioned these groups, including quasi-Boryokudan, as Anonymous and fluid criminal groups, and are fundamentally reviewing the existing organized crime countermeasures focused on Boryokudan, and have been promoting strategic clarification and control of Anonymous and fluid criminal groups.

---

*1 For other transactions, they are described in "Section 3. 2. (2) Major Transactions Misused for Money Laundering" in this NRA-FUR.

*2 Executive Order 13581 of July 24, 2011

(B) Characteristics

Anonymous and fluid criminal groups have the following characteristics:

- Anonymity of core members and fluidity of crime actors

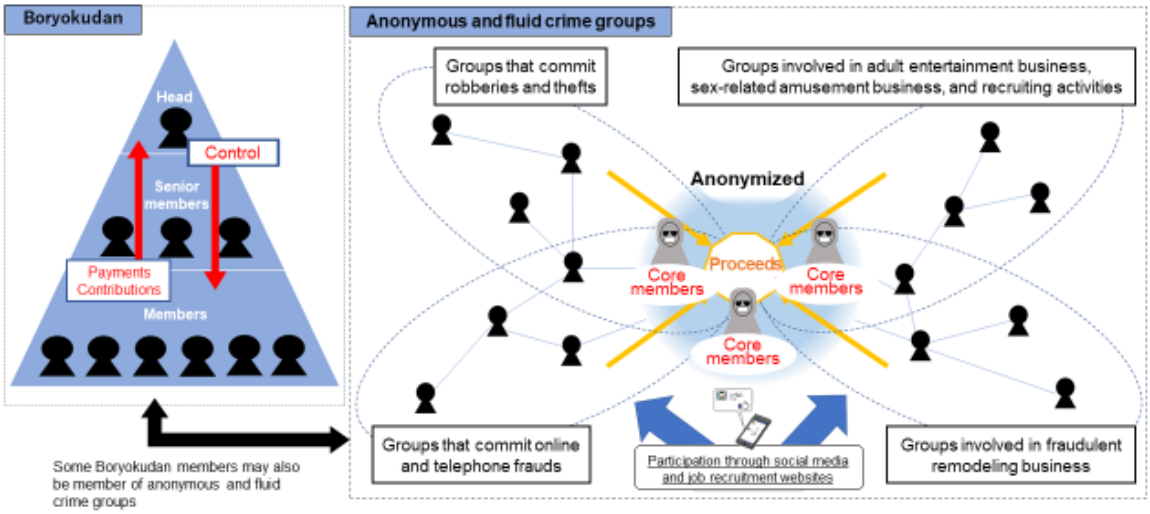
To avoid investigations reaching themselves, core members who collect proceeds from various crimes are anonymized by using highly anonymous means of communication to give instructions to crime actors, while crime actors are recruited on social media each time, and new actors are recruited even after arrests are made, making them fluid.

- Diverse fundraising activities and the return of criminal proceeds

They commit a variety of crimes, including online and telephone fraud, organized armed 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 criminal proceeds, such as by using funds acquired through crime for new fundraising activities such as adult entertainment.

It has also been confirmed that some of the 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. There are some relationships between Boryokudan and Anonymous and fluid criminal groups, and it appears that there are also individuals who act as hubs between the two.

Table 10: Characteristics of Boryokudan and Anonymous and fluid criminal Groups



(ii) Fundraising Crimes

Regarding the fundraising crimes[*1] believed to be committed by Anonymous and fluid criminal groups from April to May 2024, looking at the 508 people arrested for main fundraising crimes[*2] by type of crime, there were 289 fraud cases, 34 robbery cases, 103 theft cases, 70 drug-related offences, and 12 violation of the Amusement Business Act, suggesting that Anonymous and fluid criminal groups use fraud as their main source of funds.

(A) Online and telephone fraud[*3]

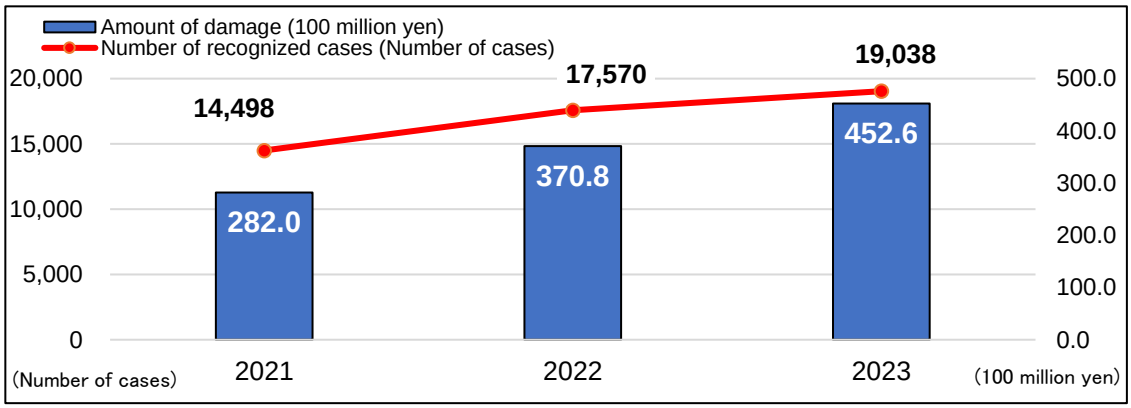
In recent years, there has been a situation where online and telephone frauds, believed to be carried out by Anonymous and fluid criminal groups, are being conducted on a wide scale. Criminal groups committing online and telephone frauds are increasingly downsizing and diversifying their bases, such as scam operation bases, and relocating them at short intervals. There are also cases where the masterminds, instructors, callers, and scam operation base are located in foreign countries.

[Topic] Recent Situation concerning Online and Telephone Fraud

1. Number of Recognized Online and Telephone Fraud Cases

The number of recognized cases of online and telephone fraud and the amount of damage in 2023 continued to increase from the previous year, and the situation remains serious (increased 8.4% and 22.0%, respectively, compared to the previous year).

Table 11: Number of Recognized Online and Telephone Fraud Cases and Amount of Damage



2. Modus Operandi of Online and Telephone Fraud

The number of recognized online and telephone fraud cases and the amount of damage by main modus operandi are shown in the following tables:

[*1] Fundraising 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, armed 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, armed robbery, theft, drug-related offences, and violation of the Amusement Business Act.

[*3] 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.

Table 12: Number of Recognized Cases by Modus Operandi

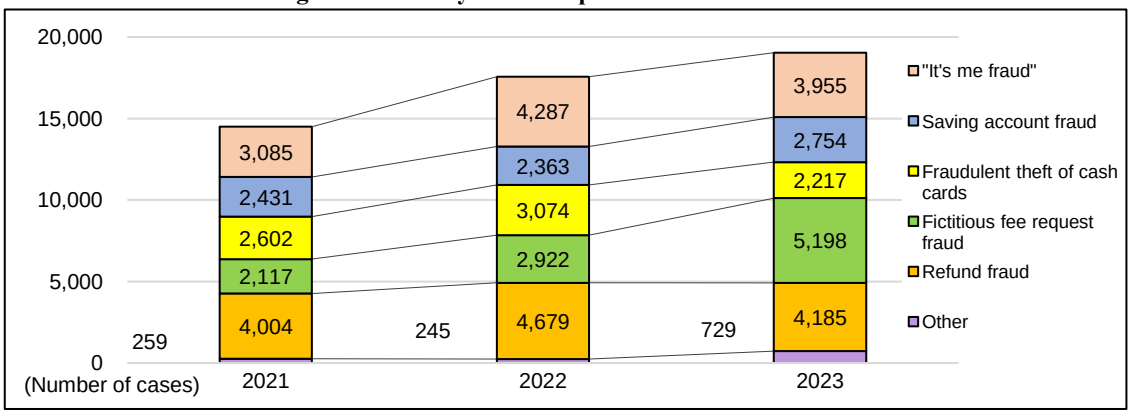
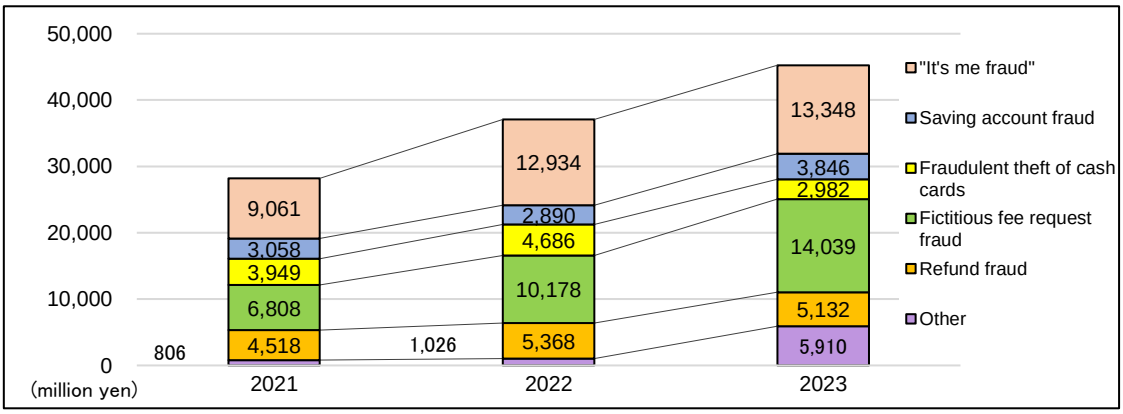


Table 13: Amount of Damage by Modus Operandi



3.Recognized Cases by the Form of Payment of the Damage

The forms of payment for these frauds 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 transfers, cash mailing, and electronic money.

The number of recognized cases and the amount of damage by the form of payment are shown in the following tables:

Table 14: Number of Recognized Cases by Form of Payment

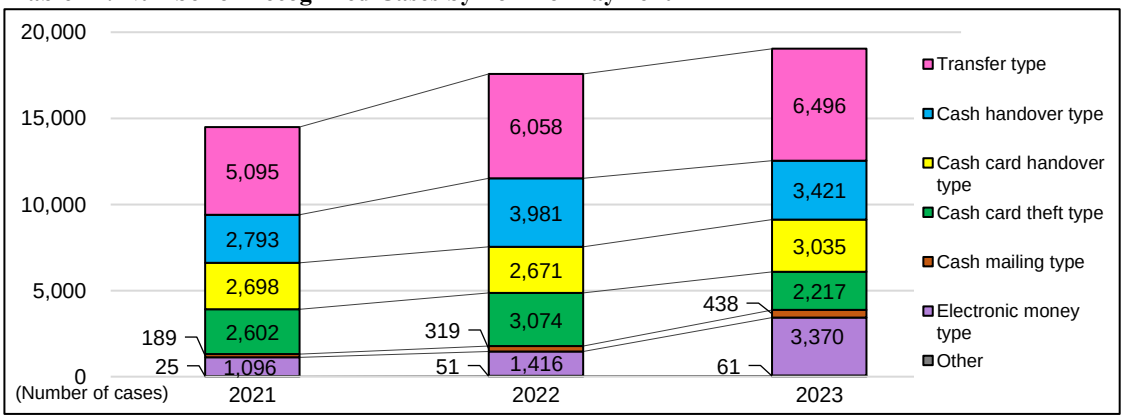
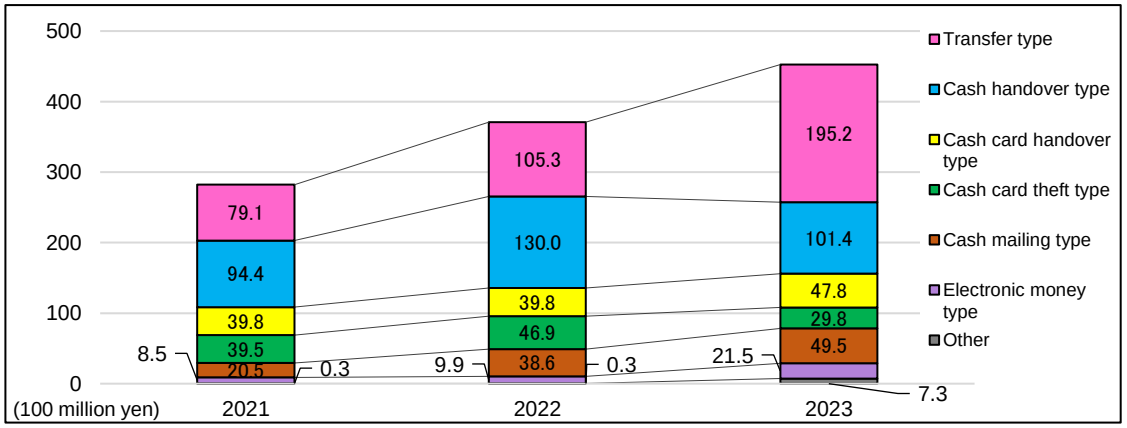


Table 15: Amount of Damage by Form of Payment



(B) Investment /romance fraud via social media[*1]

In the second half of 2023, the number of victims of investment /romance fraud via social media increased sharply, with the amount of damage during the year reaching approximately 45.5 billion yen, exceeding the amount of damage from online and telephone fraud (approximately 45.3 billion yen), making the situation extremely alarming.

Table 16: Status of Damage from Investment / Romance Fraud via social media in 2023

	Number of recognized cases	Amount of damage (yen)
Investment fraud via social media	2,271	Approximately 27.79 billion
Romance fraud via social media	1,575	Approximately 17.73 billion
Total	3,846	Approximately 45.52 billion

Looking at the status of damage during 2023, the following characteristics were observed:

- The average damage per case exceeds 10 million yen.
- The majority of victims are men in their 50s and 60s, and women in their 40s and 50s.
- In many romance fraud via social media cases, the pretext is investment.

Investment / romance fraud via social media are typical modus operandi used by Anonymous and fluid criminal groups, and necessary measures are being promoted in terms of both control and prevention.

(C) Armed robbery and theft (organized theft)

It is also apparent that armed robbery and theft are conducted after the actors are recruited by using phrases such as "high-paying part-time work" and "instant cash" on social media or job sites. From September 2021 to March 2024, 78 cases of armed robbery and theft, conducted through modus operandi that are believed to

*1 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, creates romantic feelings and feelings of intimacy, and defrauds the victim of money.

be of Anonymous and fluid criminal groups have occurred in 22 prefectures. Some of these crimes are heinous, with victims being restrained and assaulted.

Furthermore, in recent years, organized crimes of metal thefts[1], vehicle thefts and shoplifting have become growing security challenges. These crimes are often committed by groups of foreign nationals and other criminals, and the stolen goods are illegally exported to foreing countries(see Table 17).

As for metal theft, the number of recognized cases increased approximately 1.6 times compared to the previous year, and it appears that stolen copper wire and other metals are sold to buyers and illegally exported to foreign countries, suggesting the existence of malicious yards in this process.

Regarding vehicle theft, although the number of recognized cases had been on a downward trend since 2003, it started to increase in 2022. There have also been confirmed cases where stolen cars are taken to malicious car dismantling yards, dismantled, and then illegally exported to foreign countries.

As for shoplifting, there are also serious incidents such as organized mass theft by Vietnamese groups. The stolen goods are then transported back to the offenders' home countries and then sold at inflated prices, generating illegal profits. The presence of instructors abroad has also been confirmed.

In these cases, various individuals are involved in the entire process from the crime to the disposal of the stolen goods, and some cases cross borders. As such, the National Police Agency has established a "Working Group for the Promotion of Measures against Organized Theft and Distribution of Stolen Goods" to conduct cross-sectoral reviews and implement comprehensive measures for investigation and prevention.

Table 17: Recognized Cases of Metal Theft and Vehicle Theft

Year / Category	2021	2022	2023
Metal theft	7,534	10,368	16,276
Vehicle theft	5,182	5,734	5,762

(D) Financingactivities in bustling areas and nightlife spots

Activities in bustling areas and nightlife spots, such as direct and indirect involvement in the management, scouting and other operations of amusement businesses, sex-related businesses, gambling businesses, and other such businesses,are thought to be major sources of financing for anonymous and fluid criminal groups. These groups are now strengthening their resistance to the police while covering up what they are actually doing and how their funds flow-for example, by making use of highly anonymous means of communication.

Recent years have seen another type of issue come to the fore, namely male employees of “host clubs” and similar establishments demanding thar their female guests pay hefty bills for the employees entertaining them and then forcing them to work as prostitutes or to work for sex-related businesses to pay such bills. Some of these host clubs and similar establishments operate without a business license issued in accordance

[1] Refers to theft in which the stolen goods are metal items (copper sheets, copper wire, drain covers, manholes, etc.).

with the Act on Control and Improvement of Amusement Business or engage in illegal activities even when they are licenced, such as violations of rules concerning custom solicitation, business hours, indication of charges, and so forth. There are also concerns about the possibility that organized crime groups and anonymous and fluid criminal groups are unfairly profiting in the background.

While keeping an eye on the possible involvement of such criminal organizatons, the police are implementing strict crackdowns on un scrupulous host clubs and similar establishments that are commiting illegal acts.

(E) Other fundraising crimes

○ Gambling offences related to online casinos

It has been pointed out that the number of Japanese people accessing overseas online casino sites 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. Gambling offences related to online casinos have actually resulted in arrests.

Table 18: Status of Cleared Cases of Gambling Offences Related to Online Casinos*[1]

Year / Category	2021	2022	2023
Number of cleared cases	16	10	13
Number of offenders arrested	127	59	107

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. 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.

○ Fraud and specified commercial transactions by malicious remodeling businesses

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, 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.

○ Drug-related offences

It has also been confirmed that Anonymous and fluid criminal groups are raising funds through the illicit trafficking of marijuana and other drugs and through loan sharking. The police are conducting thorough investigations into these fundraising activities, clarifying the facts, and promoting control.

*[1] In addition to cases where gamblers directly connect to online casino websites using computers from their homes to place gambles, cases where gamblers use computers installed in gambling parlors to play games distributed by online casino website operators and place gambles are counted as gambling offences related to online casinos.

(iii) Money laundering

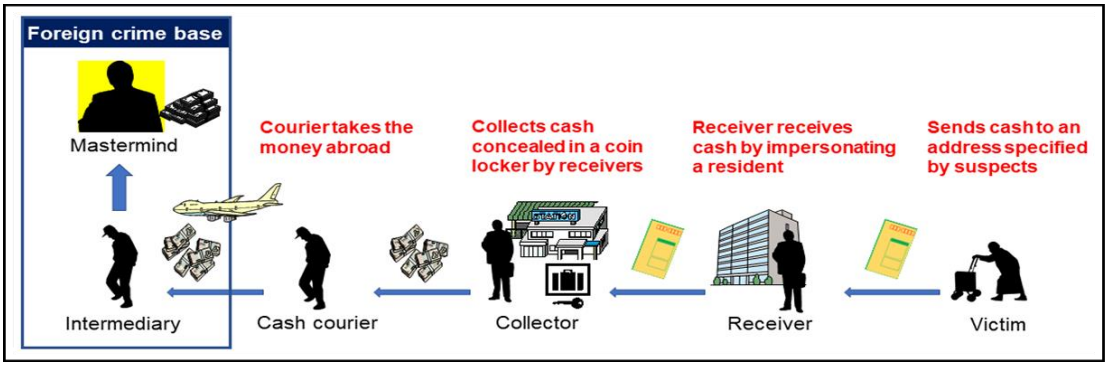
Anonymous and fluid criminal groups are skillfully conducting ML of the criminal proceeds they have obtained.

The modus operandi include:

- Transfer money using accounts under the names of fictitious or other parties (individual names, legal person's names, individuals with trade names, accounts sold by foreigners when they return to their home countries, etc.)
- Sell goods that are criminal proceeds by impersonating others
- Use coin lockers to hand over criminal proceeds
- Transfer money to a cryptoassets exchange service providers' financial institution account and deposit it into an account managed by the criminal
- Sell illegally obtained electronic gift cards (prepaid payment instruments) through websites that mediate the sale of such gift cards and depositing the sales proceeds into an account controlled by the criminals.
- Use a vacant house or room, having the victim mail cash there, and then receive it by pretending to be the recipient
- Transfer Japanese yen, which is the criminal proceeds, to a domestic account to exchange for foreign currency held by an individual

In addition, there have been cases of online and telephone fraud being committed from bases abroad, with criminal proceeds being transferred via foreign accounts, or by couriers (import/export of cash and other payment instruments) to foreign countries.

Table 19: The Conceptual Image of Flow of Criminal Proceeds Being Transferred to Foreign Countries



The ultimate destination of criminal proceeds is core members, such as masterminds and leaders of criminal groups. Therefore, it is important to thoroughly track and analyze the flow of funds within Anonymous and fluid criminal groups, and to strengthen cooperation and information sharing with relevant departments, the prefectural police, and other relevant organizations.

(3) Crime Groups of Foreigners*1 in Japan

Criminal proceeds from offences in which foreigners are involved are difficult to trace because they are transferred across borders between countries with different legal and transaction systems. Furthermore, in recent years, there have been many cases in which domestic criminals, under instructions from instructors in foreign countries, have committed theft (shoplifting) and fraud in an organized manner, exported stolen goods, and remitted criminal proceeds to foreign countries, and these crimes continue to be committed across borders.

Of the cleared ML cases in 2023, 96 cases (10.6%) were committed by foreigners in Japan.

Table 20: Number of Cleared ML Cases Committed by Foreigners in Japan

Category \ Year	2021		2022		2023	
	Number of cases	Percentage to total (%)	Number of cases	Percentage to total (%)	Number of cases	Percentage to total (%)
Number of cleared cases by foreigners in Japan	91	14.4	108	14.9	96	10.6
Related to the Act on Punishment of Organized Crimes	91	14.6	103	14.5	93	10.5
Related to the Anti-Drug Special Provisions Act	0	0.0	5	29.4	3	14.3

An analysis of status of cleared ML cases committed by foreign nationals visiting Japan from 2021 to 2023 revealed the following:

- By nationality, the majority of offenders are from China and Vietnam, with China accounting for nearly half of the total.
- By predicate offences, fraud is the most common, followed by theft and violation of the Immigration Control and Refugee Recognition Act. In terms of the type of transaction, domestic exchange transactions are the most common, followed by credit card transactions and prepaid payment instruments.
- Among ML offences that involve the misuse of domestic exchange transactions and deposit transactions, over 50% use bank accounts under fictitious foreign names or other foreigners' names.

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 in the last three years, Vietnamese nationals accounted for approximately 70% of the total.

In addition, with respect to the number of STRs in the last three years, STRs related to Vietnamese and Chinese ranked the highest among other nationalities. Recent trends of crimes committed by foreigners in Japan are as follows:

[Topic] Recent Situation Concerning Crimes Committed by Foreigners in Japan

Looking at the situation regarding arrests of foreigners in Japan committing crimes (arrests under the Penal Code and special law), both the number of cases and the number of persons arrested in 2023 increased compared to the previous year. By nationality, Vietnam and China accounted for the highest proportions of both the number of cases and the number of persons arrested (see Table 21).

*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.

The amount of loss from offences against property by foreigners in Japan arrested in 2023 was about 3.24 billion yen (an increase of 1.34 billion yen compared to the previous year), of which about 2.8 billion yen (86.8%; an increase of 1.4 billion yen compared to the previous year) was from theft, and about 365 million yen (11.3%; a decrease of 135 million yen compared to the previous year) was from intellectual crimes.

Table 21: Status of Cleared Cases by Nationality

	Number of cleared cases	
	Number of cases	Percentage (%)
Total	18,088	100.0
Vietnam	7,950	44.0
China	2,980	16.5
Thailand	856	4.7
Philippines	743	4.1
Brazil	718	4.0
Nepal	420	2.3
Cambodia	415	2.3
South Korea	399	2.2
Indonesia	380	2.1
Sri Lanka	306	1.7
Other	2,921	16.1

	Number of offenders arrested	
	Number of offenders	Percentage (%)
Total	11,534	100.0
Vietnam	4,229	36.7
China	2,008	17.4
Philippines	637	5.5
Thailand	585	5.1
Brazil	532	4.6
Nepal	377	3.3
South Korea	320	2.8
Indonesia	290	2.5
Sri Lanka	278	2.4
Cambodia	201	1.7
Other	2,077	18.0

1. Situation of Crimes Committed by Vietnamese Nationals in Japan

There are approximately 570,000 Vietnamese as foreign residents*[1] in Japan, making up about 17% of all foreign residents. By status of residence, there is an increasing trend for those with "Technical Intern Training," "Specified Skilled Worker," and "Engineer/ Specialist in Humanities/ International Services," and some individuals with bad behavior are forming criminal organizations through social media.

Among cleared cases of crimes committed by foreigners in Japan, crimes committed by Vietnamese nationals in Japan are the most common both in terms of the number of cases and the number of persons arrested. In recent years, thefts have consistently accounted for the highest percentage of crimes committed by Vietnamese, and shoplifting has accounted for the highest percentage in the method of theft. In addition, there has been a trend toward increasing intellectual crimes in recent years, and there have been many cases of mobile phone fraud at mobile phone sales agencies.

Looking at the cleared ML cases by type of predicate offences, fraud is the most common at 30.2%, followed by theft at 19.8%, and violation of the Immigration Control and Refugee Recognition Act at 14.6%. Additionally, when looking at the types of transactions misused, domestic exchange transactions are the most common at 38.2%.

Examples of cleared ML cases include the following:

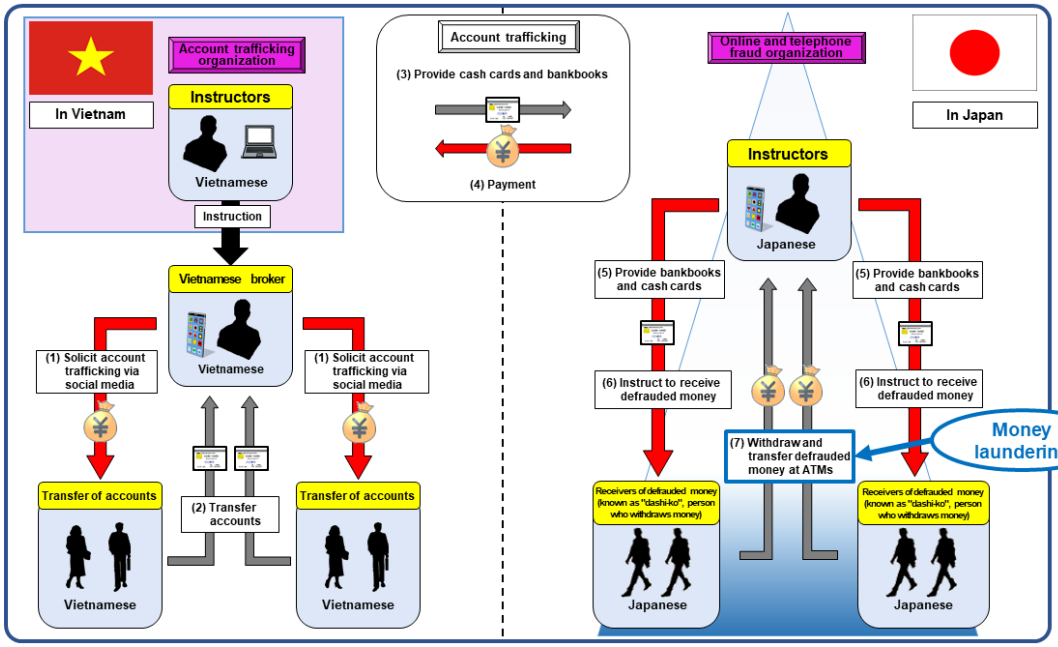
- ○ The offenders accepted requests for cross-border remittances via social media, had the money transferred to accounts under the names of fictitious or other parties in Japan, and then transferred the amount converted into the local currency from funds prepared in the foreign country to the account in the foreign country specified by the client, thus operating an underground bank.
- ○ Using illegally obtained online banking login passwords, the offenders transferred money from accounts under the names of fictitious or other parties under their control to other such accounts, and then withdrew the cash.
- ○ Sending stolen cosmetics and other items to disposal agents, falsifying the product name and sender on the shipping label.

*[1] According to the Immigration Services Agency of Japan's statistics on foreign residents as of the end of December 2023. The term "foreign residents" refers to medium to long-term residents and special permanent residents. The same applies to the rest of this section.

The existence of Vietnamese account trafficking organizations has also become evident, and in recent years, account trafficking by Vietnamese through social media has tended to increase in number. Sold accounts have been misused for various crimes including online and telephone fraud, as well as ML.

Table 22: Example: Organized account trafficking by Vietnamese

A case where a Vietnamese visiting Japan, at the instruction of a Vietnamese person living in the home country, sought persons wishing to traffic in bankbooks and cash cards via social media, purchased their bankbooks, etc., that were sent by mail, and sold them to a Japanese online and telephone fraud organization



2. Situation of Crimes Committed by Chinese Nationals in Japan

There are approximately 820,000 Chinese nationals residing in Japan, constituting about 24% of all foreign residents.

Chinese criminal organizations often form groups using regional and familial ties or by recruiting colleagues from their workplaces. There are also organizations like the Chinese Dragon, mainly composed of children of Japanese orphans left behind in China, which are expanding their influence, especially in the metropolitan areas. Recently, there have been instances of Chinese criminal organizations recruiting residents through social media to partake in criminal activities.

Among cleared cases of crimes committed by foreigners in Japan, crimes committed by Chinese nationals in Japan are second to those committed by Vietnamese nationals both in terms of the number of cases and the number of persons arrested. Looking at the types of Penal Code offences, theft accounts for 48.8%, intellectual crime for 19.8%, and violent crimes for 15.8%.

Looking at the cleared ML cases by type of predicate offence, theft is the most common at 41.8%, followed by fraud at 39.2%, and computer fraud at 10.5%. When examining the types of misused transactions, credit card misuse is the most common at 30.1%, followed by prepaid payment instruments at 13.5%.

Examples of cleared ML cases include the following:

- ○ An offender received goods that were purchased with unlawfully obtained credit card information by impersonating a holder.
- ○ An offender created counterfeit cash cards using information obtained through skimming and used them to transfer money to bank accounts under the names of fictitious or other parties.
- ○ The offender had the fraud victims transfer the fraudulent money to accounts under the names of fictitious or other parties managed by the offender, and then transferred an amount including the fraudulent money to the account of a

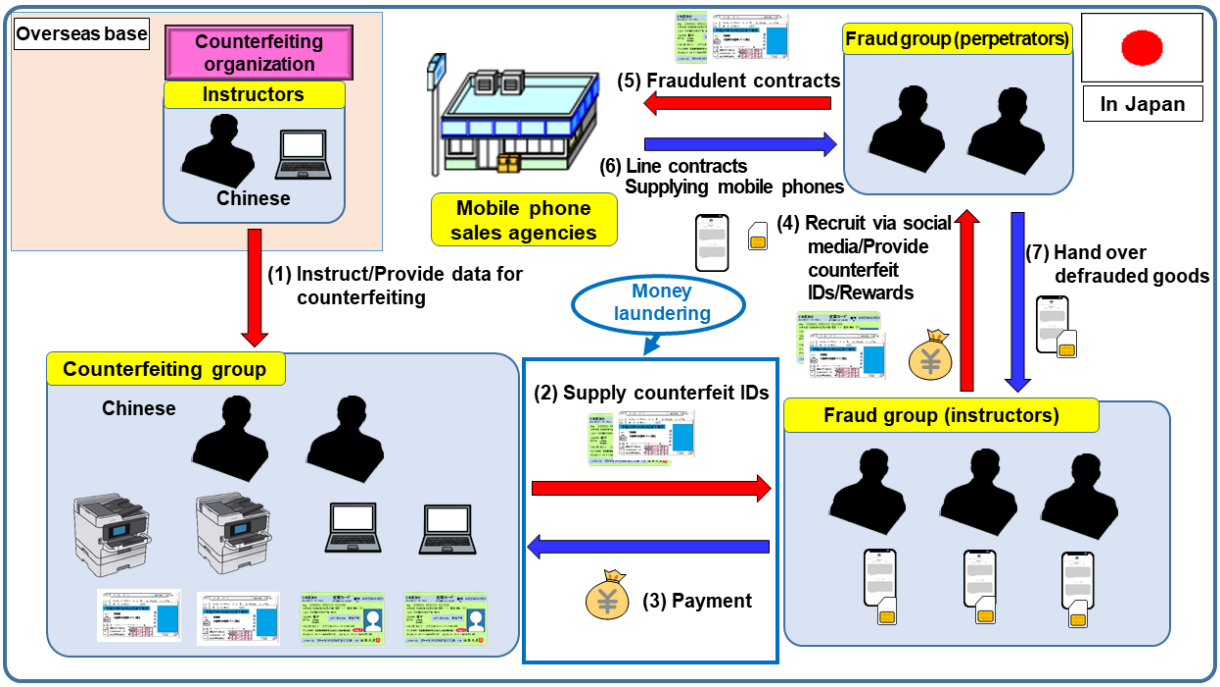
person who had requested personal foreign currency exchange, also under fictitious or other parties' names.

○ Products were purchased in stores and fraudulently obtained, using illegally obtained electronic money rights (prepaid payment instruments), impersonating the holder.

The existence of an organization made up of Chinese nationals forging ID documents has also become evident, and the manufacturers, many of whom are illegally overstaying in Japan, are recruited through social media. The forged identification cards are sent by mail to clients (Vietnamese, etc.) located throughout Japan and used to commit fraud, such as by defrauding mobile phones at mobile phone sales agencies, and are also supplied to illegal workers and used for various other crimes. In some cases, offenders have been arrested for ML after they were caught transferring the money for the transfer of the forged identification cards into accounts under the names of fictitious or other parties.

Table 23: Example: Case of forged ID documents by Chinese

A case where driver's license and residence cards were forged in an apartment in Japan, receiving instructions and personal identification data of clients from a Chinese instructor



3. Other Examples of Money Laundering Cases Involving Foreigners in Japan

○ Nigerians and others deceived a company in the U.S. into transferring money to a business account opened in Japan by sending fake emails, and pretended to have received the money in a legitimate transaction.

○ Nigerians and others deceived victims whom they met through social media into transferring money to bank accounts under the names of fictitious or other parties opened in Japan.

○ A Burmese national operated an underground bank by accepting requests for cross-border remittance and having the requesters transfer cash into bank accounts under names of fictitious or other parties opened in Japan.

○ Filipinos had victims transfer the stolen money from online and telephone fraud to accounts under the names of fictitious or other parties managed by the offenders, and then withdrew it from ATMs the same day.

2. Modus Operandi

(1) 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. Such acts are defined as crimes under the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act. Predicate offences include offences that generate illegal proceeds 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. Predicate offences that generate criminal proceeds are the threat of ML/TF in Japan.

The number of cleared ML cases categorized as predicate offences in 2021–2023[*1] is as follows:

Table 24: 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	Violation of the Investment Act/Money Lending Business Act	Drug-related offences (Note 2)	Habitual gambling/ running a gambling venue for	Violation of the Immigration Control and Refugee	Violation of the Amusement Business Act	Violation of the Trademark Act (Note 3)	Document forgery offences (Note 4)	Other	Total
2021	243	217	42	26	9	12	16	14	8	4	57	648
2022	254	257	105	13	21	11	7	4	10	12	59	753
2023	334	319	160	16	22	17	6	9	9	9	54	955
Total	831	793	307	55	52	40	29	27	27	25	170	2,356

Note 1: Money Lending Business Act (Act No. 32 of 1983)
2: Drug-related offences refer to stimulant offences, cannabis offences, narcotics offences, psychotropics offences, and opium offences.
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.

In terms of the number of cleared cases over the past three years by predicate offences, the top two crimes, fraud and theft, accounted for approximately 70% of the total, and computer fraud is on the rise.

The size of generated criminal proceeds, relevance to ML offences, types of misused transactions, danger of fomenting organized crime, and impact on sound economic activities differ depending on the type of predicate offence. It was found that Boryokudan or international crime organizations were involved in some of the predicate offences.

Major predicate offences are analyzed below, in terms of how the criminal proceeds are transferred in transactions handled by specified business operators and other business operators.

---

*1 There were 2,267 cleared ML cases under the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act from 2021 to 2023, while the total number of cleared ML cases counted by predicate offences was 2,356. This is because some ML cases that are counted under multiple predicate offences.

(i) Theft

(A) Forms of Offences and Criminal Proceeds

Thefts have a variety of modus operandi such as burglary, vehicle theft, shoplifting, some of which result in relatively small amounts of damage. However, there are also cases where online and telephone fraud methods, such as cash card fraud and withdrawal theft using stolen cash cards to withdraw cash from ATMs, are repeatedly and continuously carried out by criminal organizations, such as Boryokudan, Anonymous and fluid criminal groups, and Crime groups of foreigners in Japan, generating large amounts of criminal proceeds.

The amount of damage from theft during 2023 was about 72.6 billion yen (about 18.2 billion yen for the amount of damage in cash), generating a large volume of criminal proceeds.

(B) Money laundering cases

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

- Having an acquaintance exchange the cash (large amounts of coins) obtained through theft at a financial institution, and then having the money transferred to an account in the offender's name under the guise of a transfer from the acquaintance.
- Cases where an offender used a flea market app to sell stolen goods using an account under the name of fictitious or other party and made buyers transfer payments to an account under the name of fictitious or other party opened at a financial institution.
- Selling metals (copper wire, etc.) obtained through theft to metal buyers, impersonating a fictitious person, and converting the proceeds into cash.
- When selling a stolen car, the offender impersonates the victim and uses forged application documents to change the title to the offender's name in advance, then pretends to be the legitimate owner and sells the car to a car buyer to obtain cash.
- Using cash cards obtained through theft to operate ATMs, transferring money to bank accounts under the names of fictitious or other parties controlled by the criminals, and then withdrawing cash.

(ii) 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 2023, among property crimes (robbery, extortion, theft, fraud, embezzlement, and misappropriation of lost property), fraud accounted for the highest amount of financial damage, approximately 162.6 billion yen (with about 148.6 billion yen in cash damages). The average amount of financial damage per case of fraud was about 3.53 million yen, which is higher than the average theft case (about 150,000 yen).

(B) Money laundering cases

ML offences with fraud as the predicate offence include the following cases:

- Cases where the fraudulent proceeds from a victim through romance fraud via social media are transferred to an account in the offender's name, then are deposited in a cryptoassets wallet at a

cryptoassets exchange service providers, after which an accomplice logs into the criminal's account to purchase and transfer the cryptoassets.

- Cases where the fraudulent proceeds of online and telephone fraud are transferred from a victim to accounts under the names of fictitious or other parties managed by the offender, and then transferred to another accounts under the names of fictitious or other parties.
- Cases where housing loan funds are obtained through deception, using forged documents to illegitimately open bank accounts under the name of fictitious or other parties for the deposit of these funds.
- Cases where an offender opened and misused bank accounts under the name of fictitious or other parties to receive criminal proceeds from fraud.

In many cases, fraudulent proceeds from fraud were transferred to bank accounts under the name of fictitious or other parties, as described above.

(iii) Computer fraud

(A) Forms of Offences and Criminal Proceeds

Computer fraud includes illegal remittance offences in which offenders use IDs and passwords for online banking to illegally access the service system managed by financial institutions to transfer money from accounts under the names of fictitious or other parties to accounts managed by the offenders. It also includes the use of cash cards obtained illegally through online and telephone fraud to make transfers to accounts under the names of fictitious or other parties, and refund fraud, which is one of the modus operandi of online and telephone fraud.

In 2023, both the number of online banking fraud cases and the amount of damage were the highest ever[*1].

(B) Money laundering cases

ML offences with computer fraud as the predicate offence include the following cases:

- Cases where a criminal organization in China illegally accessed a system of a financial institution in Japan by using IDs and passwords for online banking belonging to others and transferred money to an account under fictitious or other party’s name managed by the offenders to allow a Chinese criminal group in Japan to withdraw cash from the account.
- In an online and telephone fraud under the pretense of a refund, the victim is tricked into operating an ATM without realizing that it is a remittance operation, and the offender makes the victim transfer money to accounts under the names of fictitious or other parties managed by the offender.
- Cases where an offender illegally used an electronic money payment app that was installed in a smartphone illegally obtained by the offender and deposited money into the electronic money rights from the bank account linked to the account in the app by impersonating the owner of the smartphone.

---

*1 For details on the number of victims in 2023, please refer to "Section 2. 4. (1) (ii) (B) Situation of Online Banking Fraud Cases" in this NRA-FUR.

(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 loan-shark crime[*1] whereby a money lending business operates without a registration and lends money at a high interest rate. The modus operandi include instances of lending without the lender and borrower directly meeting, where the borrower returns money by transferring it to accounts under the names of fictitious or other parties. Lenders may send direct mails based on the personal information described in lists of heavy debtors or solicit an unspecified large number of persons through online advertisements or phone calls. Recently, there have been cases called "Deferred payment monetization," where offenders enter into a sales agreement for goods with victims under deferred-payment terms to lend money as compensation for advertisement of the goods sold and collect money from the victims by calling it a payment for the goods. Additionally, there are cases known as "Upfront purchase monetization," where a formal sales contract for a product is concluded, and money is lent as the purchase price in advance. Subsequently, under the pretext of contract cancellation due to the customer's circumstances, repayment of the purchase price is demanded, along with the receipt of a high amount of interest as a penalty.

The amount of loss from loan-shark crime committed by offenders who were arrested in 2023 exceeded 23.3 billion yen, generating a large amount of criminal proceeds.

(B) Money laundering cases

ML offences involving loan-shark crimes as predicate offences include the following cases:

- Cases where debt repayments were remitted to accounts under the name of fictitious or other parties to conceal debt repayments to the loan sharks.
- Cases where an offender made use of credit card payment to requires victims to pay debts.

Accounts under the names of individuals owing debts who transferred their accounts to loan sharks in return for payment of debts owed by such individuals were used as accounts for hiding criminal proceeds from these debt payments.

In addition, there have been cases, including the following ones where:

- When obtaining repayments from borrowers, the offenders disguise the payments as legitimate business revenues (such as purchase refunds or penalty fees) from breach of contracts in the sale of goods, and have the repayments transferred to legal persons' accounts managed by the offenders.
- The offenders operate a money lending business under the guise of operating a flea market website, lending money to customers posing as sellers by transferring money to their accounts under the pretense of purchasing gift certificates, and then have the gift certificates delivered in an amount equal to the loan amount plus the illegal amount of interest.
- Loan sharks made a borrower transfer repayments to other borrower's account and made the second borrower send all or part of the repayments to other borrower to lend money to the third borrower.

---

*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 rate, 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) 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"). In particular, regarding the promotion of illegal employment, there are cases of trafficking in persons 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 manufacturing bases once located in China have been established within Japan. Under the direction of instructors based in China, various nationalities of residents, including Chinese nationals, were recruited to manufacture forged residence cards. Since the instructors are located in China, even if manufacturing bases within Japan are exposed and dismantled, they continue to establish new manufacturing bases using similar methods. This type of offences tend to exhibit a high degree of organization.

In 2023, there were cases where an organized counterfeit residence card factory operated by a group comprising Japanese, Chinese, and Vietnamese individuals was exposed and dismantled.

(B) Money laundering cases

ML offences involving a violation of the Immigration Control and Refugee Recognition Act as a predicate offence include the following cases:

- Cases where an offender made purchasers of forged residence cards pay for the cards by transfer to accounts under the names of fictitious or other parties.
- Cases where an offender received compensation for introducing foreigners remaining in Japan to employers after the expiration of their authorized period of stay as rental income under fictitious residence lease agreements.

(vi) 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 online casino gambling, in addition to hanafuda gambling, baseball gambling, and game-machine gambling. The reality is that Boryokudan are deeply involved, 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 agent for bets was arrested for aiding habitual gambling.

In the last three years, the number of cases of temporary restraining order for confiscation before institution of prosecution prescribed by the Act on Punishment of Organized Crimes has been high for habitual gambling/running a gambling venue for profit. In 2023, the orders for confiscation were issued against about 6.36 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 the following cases:

- ases where a person who acted as a payment agent for an online casino made a customer transfer money from his/her own account to an account in the name of a legal person managed by the offender as payment for the purchase of points for gambling at the casino, and then transferred the money to another account in the name of a different legal person.
- Cases where individuals knowingly receive cash under the pretext of leasing gaming machines, knowing that it is part of the proceeds of a criminal act in a gambling establishment.

In addition, there was a case where criminal proceeds obtained via gambling offences were processed as legal business proceeds using an innocent certified public tax accountant, etc.

(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 (Act No. 158 of 1956), the reality is that Boryokudan have been directly or indirectly involved in certain cases. Examples include association with operators of illegal amusement businesses or sex-related businesses (hereinafter, "amusement business,etc."). Criminal proceeds from these offences are an important source of funds for them.

In addition, the following trafficking in persons cases have also been observed:

- Cases where foreigners who were staying illegally in Japan worked in the amusement business
- Cases where offenders forced victims who are foreigners to engage in prostitution by using violence, and intimidation
- Cases where employees of a host club forced female customers to engage in prostitution in order to make them pay accounts receivable for meals.

In the last three years, the number of cases of preservation order for confiscation before prosecution prescribed by the Act on Punishment of Organized Crimes has been high for violation of the Amusement Business Act and the Anti-Prostitution Act. In 2023, there was a case where bank deposit claims of approximately 6.06 million yen, which were the proceeds made in violation of the Amusement Business Act, became subject to 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 following cases:

- Cases where an offender made customers at an unlicensed restaurant offering entertainment service pay for meals with a credit card payment terminal installed at another restaurant owned by the offender, and then has the sales proceeds transferred to an account in the name of an acquaintance through a credit card payment agency to receive the proceeds.
- Cases where a Boryokudan member received criminal proceeds from prostitution through a bank account under the name of a family member.
- In order to collect accounts receivable from a customer of a host club for meals, the offender made a customer work in a "bathhouse with private rooms" and engaged in prostitution, and then had the customer transfer the proceeds to an account the offender managed, knowing that the proceeds were criminal proceeds from prostitution.

(viii) Drug-related Offences

(A) Forms of Offences and Criminal Proceeds

The following characteristics are observed regarding drug-related offences in Japan.

- Looking at the amounts seized and the amounts seized from smuggling (see Table 25), smuggling and illegal trafficking of drugs still generates a large amount of criminal proceeds.
- The number of arrests for stimulant drug smuggling offences in 2023 was 200, an increase from the previous year. In addition to the persistent domestic demand for stimulants, drug-related crime organizations with international networks exist both domestically and abroad, which are considered to be intensifying stimulant drug trade.
- Looking at the status of cleared cases of profit-making offences by type of drug-related offence (see Table 26), the proportion of Boryokudan gangsters in profit-making stimulant offences exceeds 30%, and there has been a significant increase in drug-related offences committed by foreigners for profit-making purposes, suggesting the involvement of Boryokudan and foreign criminal organizations.
- Boryokudan are deeply involved in the distribution process of stimulants (shipping from foreign countries, receiving consignments, wholesale, intermediate wholesale, and end-user illicit trafficking) in collusion with foreign drug trafficking organizations, considering the fact that Boryokudan gangsters and Taiwanese nationals were arrested alongside in a smuggling case in 2019, in which 587 kilograms of stimulants were seized.
- Criminals are likely to move criminal proceeds related to the trafficking or smuggling of drugs between countries that have different legal and transaction systems.
- The number of cases of preservation order for confiscation before prosecution prescribed by the Anti-Drug Special Provisions Act in 2023 was 20, targeting monetary claims totaling approximately 45.43 million yen as well as foreign currency. In the past, targets have included automobiles, land, and buildings, which means that criminal proceeds obtained in cash, etc., are transformed into another type of property.

Table 25: Trends in Amounts Seized and the Amounts Seized from Smuggling by Drug Type

	Amount seized			Amount seized for smuggling		
	2021	2022	2023	2021	2022	2023
Stimulants (kg)	688.8	289.0	1,342.9	673.1	282.1	1,215.5
Dried cannabis (kg)	329.7	289.6	784.5	8.7	13.9	370.4
Cannabis concentrate (kg)	22.2	74.0	35.7	18.3	70.2	30.9

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

Table 26: Status of Cleared Cases of Profit-making Offences by Type of Drug-related Offence

		2021	2022	2023
Stimulant offences	Number of offenders arrested	455	450	603
	Boryokudan gangsters	246	191	220
	Percentage (%)	54.1	42.4	36.5
	Foreigners	66	97	170
	Percentage (%)	14.5	21.6	28.2
Cannabis offences	Number of offenders arrested	426	436	550
	Boryokudan gangsters	104	105	112
	Percentage (%)	24.4	24.1	20.4
	Foreigners	50	40	71
	Percentage (%)	11.7	9.2	12.9

(B) Money laundering cases

ML offences involving drug-related offences as a predicate offence include the following cases:

- Cases where traffickers of stimulants had buyers make payments by transfer to a bank account under the name of fictitious or other parties.
- Cases where an offender had buyers make payments by transfer to a bank account in the name of the offender, and withdrew cash at an ATM, knowing that the payments were criminal proceeds obtained from the trafficking of cannabis.

In addition to those cases where criminal proceeds are transferred into accounts under the name of fictitious or other parties for the purpose of concealing and receiving them, there are also cases including:

- Cases where the payment system of flea market app are misused to disguise the origin of money.
- Cases where funds transfer services are used to send criminal proceeds obtained from drug smuggling to foreign countries.

(ix) Other Predicate Offences

- **Environmental crime**

The FATF points out that illegal trade in wildlife, forest resources and minerals, as well as malicious waste dumping, are among the most profitable crimes, generating approximately 110 to 281 billion US dollars in criminal proceeds each year, and are linked to many other serious organized crimes such as corruption, tax evasion and drug trafficking. It also indicates that countries need to pay attention to the point below in addressing ML[*1]:

*1 Money Laundering from Environmental Crime (July 2021)

- Even countries without domestic natural resource industries need to consider the threat of ML.
- Countries need to implement the standards required by the FATF.

Environmental crimes in Japan include waste-related crimes and animal/bird-related crimes. The number of cleared environmental cases in 2023 was 5,054 waste-related crimes (a decrease of 221 from the previous year) and 778 other environmental crimes[*1] (a decrease of 58 from the previous year). Although there have been no cleared ML cases in the past three years in which an environmental crime was used as a predicate offence, there has been a case in the past in which an individual operating an industrial waste disposal business without a license obtained criminal proceeds by accepting a contract to transport and dispose of industrial waste generated during building demolition work, and then had those proceeds transferred to accounts in other party's names.

[*1] Other environmental crimes include violations of the Forest Act (Act No. 249 of 1951), the Construction Recycling Act (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 Animal Welfare and Management Act (Act on Welfare and Management of Animals (Act No. 105 of 1973)) and the Wildlife Protection and Management Act (Act on the Protection and Management of Wildlife, and the Optimization of Hunting (Act No. 88 of 2002)).

[Topic] Flow of Criminal Proceeds from Cyber Enabled Fraud (CEF)

1. About the CEF Report[*1]

Digitalization and technological developments have fundamentally changed the environment surrounding crimes and increased the threat of cyber-enabled fraud (hereinafter referred to as "CEF"). In particular, the COVID-19 pandemic has accelerated the shift from face-to-face financial activities to online transactions. These changes in financial behavior are also affecting the ML environment, such as the increased use of online banking and payment platforms, and remote transactions. Criminals are using technology to expand the scale, scope and speed of their criminal activities, and the growing use of "Crime-as-a-Service" (CaaS) is increasing the expertise of criminal organizations that undertake the division of labor. In light of the significant increase in CEF internationally, FATF, Egmont Group and ICPO launched a joint project and published a report in November 2023, classifying CEF and pointing out the flow of criminal proceeds as shown in the table below:

(i)	Business Email Compromise (BEC[*2]) fraud	Victims receive email instructions that purport to be from their clients or suppliers' asking victims to transfer funds to new payments accounts.
(ii)	Phishing fraud	Victims are deceived into revealing sensitive information such as personal data, banking details or account login credentials. The criminal will then use the information to drain the victims' money from their payments accounts, open new payment accounts or make fraudulent transactions.
(iii)	Social media and telecommunication impersonation fraud	This includes scenarios where victims are contacted via mobile or social media applications by criminals pretending to be government officials, relatives or friends, and prey on the victims' emotions to have them make payment, hand over control of payments accounts, open an account, etc.
(iv)	Online trading/ trading platform fraud	Victims are deluded by fake advertisements or advisors online to non-existent or fake (fraudulent) platforms for trading or investment related to both fiat and virtual assets.
(v)	Online romance fraud	Victims are duped into sending money to criminals after being convinced that they are in a romantic relationship.
(vi)	Employment scams	Fake job offers on social media platforms trick victims to pay scammers upon various excuses including advanced payment for purchasing commodities to boost sales of a trading platform or a guarantee fee to secure employment.

(1) Characteristics

- ○ CEF is a growing transnational organised crime. CEF criminal syndicates are often well structured into distinct sub-groups with specialised areas of criminal expertise, including money laundering.
- ○ Aided by digitalization and advanced technology, CEF criminal syndicates use various tools and techniques to deceive victims or prey on their psychological state and emotions to extract as much funds as possible.
- ○ With the modus operandi of combining romance scam and investment fraud, criminals build a trust relationship with the victim and convince them to invest savings. The scam is perpetrated over time, resulting in the loss of large amounts of money. Following the realisation of the fraud, criminals often contact their victims posing as lawyers or law enforcement agents offering help to retrieve their funds, in exchange for a fee.
- ○ Criminals will use a variety of techniques to achieve the ultimate goal of inducing a funds transfer from victims. Criminals may engage or transition to other types of CEF if the initial deception begins to fail.

(2) Characteristics of money laundering

- ○ CEF has increased significantly internationally. Illicit proceeds from CEF are often transferred to foreign jurisdictions. These proceeds may then be further laundered through the financial systems of other third-party jurisdictions.

○ Regions that are highly cashless and digital-based are expectedly more vulnerable to the ML risks associated with this crime, although the transnational nature of CEF means that criminals can easily target victims regardless of international borders.

○ The professional ML groups may be part of the CEF criminal syndicate, or a separate de-centralised organisation that provides ML services under the "crime-as-a-service" model.

○ CEF-proceeds are rapidly laundered through a network of accounts. These networks can be complex by extending across multiple borders and financial institutions, and CEF-related ML networks of accounts typically involve individuals as well as legal entities.

○ Individual money mules[*3] are often recruited by criminals via various means, including through job offers and advertisements, as well as online social media interactions. Money mules may be knowingly complicit in the laundering of funds or work unwittingly (through deception), or negligently, and may also be offered incentives or fees to handle the illicit funds.

○ Victims of CEF (e.g., through romance fraud) can often be tricked into acting as money mules.

○ Some jurisdictions noted instances of the recruitment of foreign nationals with no apparent connection to the jurisdiction, with these individuals directed to set up mule accounts, either by physical travel or through virtual account opening.

○ Legitimate companies, similar to individual money mules, may also be tricked into receiving CEF-proceeds and asked to either re-direct the funds or be refunded into a separate criminally controlled account.

○ The type of account used to receive CEF-proceeds typically depends on the type of CEF. Changes over time have also been observed in the first layer account type. For example, in BEC fraud cases, CEF syndicates have shifted from the use of accounts of individual persons to the use of accounts of corporates to reduce the risk of detection.

○ The use of unhosted wallets, peer-to-peer transactions[*4], peel chains, etc., are the preferred methods to launder cryptoassets-related CEF-proceeds, and are often used in combination.

(3) Responses and Strategies

○ Victim reporting and suspicious transaction reports are important source of information for detecting and investigating CEF-related illicit proceeds.

○ Timely victim reporting is important to enable competent authorities to act quickly to trace illicit proceeds.

○ STRs are a vital independent source of detection for CEF-related financial flows. Most CEF-related STRs were filed by the banking sector. Banks should continue to strengthen their capabilities to detect ML, as CEF syndicates continuously evolve their modus operandi.

○ Real-time transaction monitoring, which involves the use of sophisticated software and algorithms to monitor financial transactions, is considered useful for detecting and preventing CEF.

○ The scale and magnitude of CEF is expected to grow with the rising trend of digitalisation and virtual services across the globe. Jurisdictions should be aware of the additional vulnerabilities across various sectors, including digital financial institutions, that criminals may exploit to enhance CEF and ML techniques through growing digitalisation.

○ Jurisdictions must collaborate multi-laterally to effectively and expeditiously intercept CEF proceeds that are laundered across borders.

2. Key Focus Points When Submit STRs

The risk indicators related to CEF are as follows:

---

*1 Illicit Financial Flows from Cyber-Enabled Fraud (November 2023)

*2 Business Email Compromise

*3 A method of ML. Money Mule involves utilization of a third party to carry criminal proceeds. Third parties are recruited through e-mail or recruitment websites, etc.

*4 Refers to transactions between individuals.

Indicators regarding transaction patterns
● Rapid or immediate, high or low value transactions after opening of an account, inconsistent with the purpose of the account ● Rapid or immediate cash withdrawals or transfers of large amounts following the receipt of a funds transfer in order to empty the account ● Frequent and large transactions, which are inconsistent with the account holder's economic profile ● Transfers of funds to and from high-risk money laundering jurisdictions ● Large frequent transactions with recently established companies and/or whose main activities are not consistent with the activities carried out by the beneficiary ● Small payment to a beneficiary, which once successfully completed, is rapidly followed by larger value payments to the same beneficiary ● Round value amount purchases that are frequent and/or in large amounts, which can indicate gift card purchases ● Mismatch of account number and name of the holder of the account
Indicators regarding customer transaction instructions
● A customer transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors ● A customer's seemingly legitimate transaction instructions contain a different language vernacular, timing, and amounts than previously verified transaction instructions. ● Transaction instructions include markings, assertions, or language designating the transaction request as "Urgent," "Secret" or "Confidential" ● A customer presents poorly formatted messages / emails as justification of a transaction. ● Transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used ● The intended beneficiary in the transaction description and the name of the account holder known to the beneficiary bank are inconsistent ● Transfers ordered by natural persons with no financial experience and expertise, in favour of companies (in many cases established in high-risk jurisdictions) with reasons for payments related to investments and financial products ● Counterparties incommensurate with the business/company name of the account might suggest which may provide cover for the movement of large amounts of funds internationally ● Transactions conducted with device time zone mismatch
Indicators regarding account holder/account user
● Account holder is unwilling or unable to pass CDD[*1] checks ● Account holder is unfamiliar with the source of the funds moving through their account or claiming they are transacting for someone else ● Frequent changes of legal entities'/sole proprietorships' names using foreign expressions and terminology ● The customer shows to have inadequate knowledge on the nature, object, amount or purpose of the transaction/s or relationship or provides non-realistic, confusing or inconsistent explanations, which drive to the suspicion that the customer is acting as a mule ● The user is attempting to conceal their identity by using shared, falsified, stolen or altered identification (address, telephone number, email) ● Frequent changes of contact details, phone numbers, email addresses after opening of the account ● E-mail addresses that do not seem compatible with the name of the account holder, or a pattern of similar email addresses seen across multiple accounts ● Irregularities in customer profile particulars, such as shared credentials with other accounts ● Abnormalities identified via online behaviour, such as hesitation inputting data, keystroke delays, multiple failed login attempts ● Accounts relating to entities who could be expected that they are no longer active in the jurisdiction (e.g., overseas students' account sold when completed study) ● IP addresses or GPS coordinates originating from high-risk money laundering jurisdictions ● Use of hosting companies that may mask a user's IP address ● Multiple IP addresses associated with a single online account

*1 Customer Due Diligence. Refers to customer management.

- Single static IP address associated with multiple accounts of various account holders
- Remote desktop connection access to an account through computer ports used by applications such as TeamViewer
- Accounts operated with excessively quick keystrokes or navigation suggesting possible bot control
- Presence of material relevant and verifiable negative news on customer or counterparties
- Fraud report or recall from a correspondence institution, or other 3rd party fraud databases
- Presence of wire transfers' recall requests
- Presence of adverse information provided by FIUs or LEAs about persons involved in a transaction

Indicators regarding cryptoassets transactions

- Sending/receiving large volumes or high frequency low amounts worth of cryptoassets to unhosted wallet addresses; or addresses associated with darknet marketplaces, ransomware groups, gambling sites, etc.
- No documents proving the origin of cryptoassets or of the money converted in cryptoassets
- Transfers of cryptoassets to wallets linked to illegal activities on the dark web
- Transactions involving more than one type of cryptoassets
- Abnormal transaction activity of cryptoassets from peer-to-peer platform associated wallets

(2) 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 this guidance, the police analyzed cleared ML/TF cases to examine what transactions were misused for ML/TF, summarizing 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 (if any), to the extent revealed in the course of the investigation. The results of the analysis for the three years from 2021 to 2023 are shown in Table 27.

Table 27: Major Transactions Misused for ML

Year \ Misused transactions	Domestic exchange transactions	Cash transactions	Credit cards	Deposit transactions	Prepaid payment instruments (Note 1, Note 2)	Cryptoassets	Funds transfer services	Legal persons	Cross-border transaction (such as foreign exchanges)	Precious metals and stones	Financial instruments	Real estate	Foreign currency exchange	Legal/accounting professionals	Money lending	Bills and checks	Postal receiving services	Total
2021	208	72	40	40	21	9	9	16	9	2	2	0	1	1	0	0	0	430
2022	266	105	55	24	39	16	10	6	7	1	0	0	0	1	0	0	0	530
2023	311	129	51	36	40	29	21	15	11	3	3	4	2	0	2	1	1	659
Total	785	306	146	100	100	54	40	37	27	6	5	4	3	2	2	1	1	1,619

Note 1: Since 2023, the name “electronic money” has been changed to “prepaid payment instruments” in the NRA-FUR.
2: The figures for prepaid payment in 2021 include transactions that corresponded to prepaid payment instruments within electronic money.

The results of the analysis of the cleared ML cases and STRs are as follows:

- There were 785 cases of domestic exchange transactions*[2], followed by 306 cases of cash transactions and 100 cases of deposit transactions, with the majority of transactions misused for ML involving products and services offered by deposit-taking financial institutions.
- There are many 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.
- Ultimately, the criminal proceeds deposited into accounts through domestic exchange transactions or deposit transactions are often cashed out, making subsequent fund tracing extremely challenging.
- The number of cases where credit cards were misused for ML was the third highest. With the significant

*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 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.

increase in fraudulent use of credit cards, the number of misuse cases has also risen.

- There is an observable expansion in the misuse of various payment methods, including prepaid payment instruments, cryptoassets, and funds transfer services, reflecting the diversification of payment methods.

In addition, there are also many ML cases without using the products and services of specified business operators, including the following:

- Cases where criminal proceeds were mailed under someone else's name, and where mailed criminal proceeds were received under someone else's name after being left in a vacant room or a parcel box
- Cases where criminal proceeds were sold by impersonating someone else or by asking a third party who was unaware of the situation
- Cases where criminal proceeds were concealed in coin lockers in online and telephone fraud

[Topic] APG Yearly Typologies Report 2023

Each year, the APG[*1] compiles information on the modus operandi and trends of ML from participating countries and publishes the results in the "Yearly Typologies Report" (hereinafter referred to as the "Report").

The Report published in December 2023 describes the ML situation and misused transactions in the Asia-Pacific region as follows:

[Focus area: Virtual Assets & Virtual Asset Service Providers

- ○ Fraud, theft, hacking, and ransomware arecommon illicit activity taking place through cryptoassets.
- ○ Use of cryptoassets for TF is increasing.
- ○ There has been an increase in the use of cryptoassets in Proliferation Financing, in particular by the North Korea

[Situation of ML and cleared cases in each country]

- ○ Money mules are used not only to transport cash, but also to provide accounts and transfer funds between accounts. They are recruited via social media, and victims of online job fraud and romance fraud are also used as money mules.
- ○ Underground banks continue to facilitate the laundering proceeds of various other crimes such as telecommunication fraud, online gambling, and corruption.
- ○ An offender laundered the proceeds of their drug crimes by purchasing the diamond and sought to transfer the stone to another jurisdiction under the guise of seeking a specialist valuation.
- ○ The syndicate controlled a futures company, and then set up accounts specifically for ML, and laundered money by using criminal proceeds to conduct frequent, large-volume trading in the futures markets and get high transaction charges paid to the company.
- ○ An offender deposited the criminal proceeds into accounts provided by casino operators and used them to gamble at casinos. He also withdrew cash using credit and debit cards, and purchased gold bars.
- ○ Suspects opened accounts at financial institutions, deposited the criminal proceeds, and withdrew cash using an ATM located abroad.
- ○ Offenders laundered money by creating counterfeit cards through phishing, purchasing stored value cards from coffee chain stores with the counterfeit credit cards, and then selling the stored value cards to third parties.
- ○ There are traders who accept cash from victims on behalf of criminal groups and send cryptoassets of equal value to criminal groups.
- ○ There was a criminal group that established many companies in the names of relatives and engaged in ML.
- ○ Offenders collected money from investors as investments in fake overseas funds and futures trading platform, and then used the money to buy real estate and life insurance policies to conceal the fact that it was criminal proceeds.

*1 Asia/Pacific Group on Money Laundering. It is an organization established to strengthen and promote anti-money laundering measures in non-FATF countries/regions in the Asia-Pacific region, offering support to countries/regions that are working on anti-money laundering measures. As of the end of 2023, 42 countries/regions, including Japan, are members of the APG.

3. Suspicious Transaction Report (STR)

(1) Overview and Reporting Status

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators (excluding lawyers, etc.[*1] and judicial scriveners, etc.[*2*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.

Looking at the number of STRs reported in 2023 by business type, the percentage of STRs reported by banks and other deposit-taking institutions was the largest, accounting for 73.8% (522,649) of the total STRs, followed by money lenders at 9.0% (63,954) and credit card operators at 6.5% (45,674) (see Table 28). Furthermore, the number of STRs used for the investigation by the prefectural police in 2023 was 496,093 (see Table 29). The National Public Safety Commission and National Police Agency collect, organize and analyze the STRs and provide investigative organizations other than the prefectural police[*6] 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 secret investigations, clarification of the Actual Status and investigations into tax offences.

---

*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 Meaning the investigating authorities set forth in Article 13, paragraph (1) of the Act on Prevention of Transfer of Criminal Proceeds.

Table 28: Annual Reported Number of STRs by Business Type

Category \ Year	2021	2022	2023
	Number of reports	Number of reports	Number of reports
Financial institutions	495,029	542,003	661,838
Deposit-taking institutions	411,683	435,728	522,649
Banks	390,381	414,651	498,155
Shinkin banks, credit cooperative	18,461	18,520	21,636
Labour banks	318	316	397
Norinchukin banks, etc.	2,523	2,241	2,461
Insurance companies	3,458	3,939	4,575
Financial instruments business operators	19,718	19,032	20,550
Money lenders	35,442	45,684	63,954
Funds transfer service providers	10,499	20,271	29,232
Cryptoassets exchange service providers	13,540	16,550	19,344
Commodity derivatives business operators	388	318	846
Currency exchange operators	201	430	655
Electronic monetary claim recording institutions	7	0	14
Other	93	51	19
Financial leasing operators	163	71	214
Credit card operators	34,904	41,106	45,674
Real estate brokers	4	11	18
Dealers in precious metals and stones	48	124	138
Postal receiving service providers	0	1	30
Telephone receiving service providers	0	0	0
Telephone forwarding service providers	2	1	17
Total	530,150	583,317	707,929

Table 29: Number of STRs Used for Investigative Purposes

	2021	2022	2023
Number of STRs used for investigation	353,832	373,849	496,093

(2) Examples of STR Utilization

As awareness of AML/CFT has increased throughout Japan, the number of STRs has been increasing every year, and the content of these reports has also become more substantial. In order to provide feedback to specified business operators that the reported information on suspicious transactions is being effectively used in the investigation of ML cases and their predicate offences, and to promote the understanding and efforts among specified business operators regarding STRs, the following introduces examples of cleared cases detected through STRs by the prefectural police

and examples of cases in which other investigating authorities utilized STRs.

(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	1. Account in the name of Japanese 2. Account in the name of legal persons
Reason for report	• Transfers to an unspecified number of individuals using transfers from a specific small number of individuals as the source of funds [1] • There are suspicious points in the explanation of transactions in which the amount of deposits and withdrawals is almost the same over a certain period of time, and there is suspicion that these transactions are intended to obscure the flow of funds [1] • The account was opened for receiving salary, but there is no evidence of salary receipt, and repeated transfers from the same person are withdrawn each time. No validity or rationality in the transactions [1] • There is suspicion that a third party is managing the account, such as using a different name for the transfer request when transferring money [1] • The number of transfers deviates from past transaction behavior [2]
Investigation results	It was discovered that the accounts were being used in an organized fraud case, and several people involved, including the account user, were arrested.

Business type of the reporter	Deposit-taking institution
Reported account	1. Account in the name of Japanese 2. Account in the name of legal persons
Reason for report	• The account receives large amounts of money from a legal person represented by the account holder, and the money was withdrawn each time [1] • The remittance bank requested a refund due to fraud for a remittance from abroad addressed to a legal person of which the account holder is the beneficial owner [1] • The account is the destination of funds transferred from a legal person account frozen at another bank [1] • There are suspicious points in comparison with general transaction patterns, as a large amount of unnatural transfers were used for withdrawals and remittances [1] • When requested to submit documents related to incoming remittances from abroad, a contract had not been prepared despite the large amount of money involved. Large amount transactions that deviate from annual sales [2]
Investigation results	The account user was found to be receiving computer fraud losses from abroad, and was arrested.

Business type of the reporter	Deposit-taking institution
Reported account	1. Account in the name of Japanese 2. Account in the name of legal persons
Reason for report	• Repeatedly made large cash deposits at ATMs and transferred them to cryptoassets exchange service providers [1]

*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.

	• There are multiple large transfers from a specific legal person or individual on consecutive days or in a single day, and the funds are then transferred to the legal person's account at another bank and withdrawn [2] • The actual business status of the legal person that is the account holder is unclear, and the transaction lacks rationality in comparison with its attributes and purpose of use [2] • A large amount of money has been transferred suddenly from a legal person with an unknown business status or relationship, and then the money has been withdrawn and sent to a large number of individuals. There is no rationality in the sudden increase in transaction amount [2] • There are frequent transfers from a specific legal person, and almost the same amount is withdrawn on the same day [2]
Investigation results	It was discovered that criminal proceeds from online and telephone fraud were transferred to the account in the name of the legal person, and the representative of the legal person was arrested.

(B) Fraud cases

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	• The driver's license number of the driver's license submitted as an identity verification document was found to be suspected of being forged • The phone number and email address used to apply for an account opening were the same as those of an account that had already been frozen or rejected
Investigation results	It was discovered that the account holder had attempted to open an account using a counterfeit driver's license, and the person was arrested.

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	• Large funds of unknown origin were transferred to cryptoassets exchange service providers, under a different name as transfer requestor • The entire amount of the transfer from an individual was withdrawn on the same day • Withdrawals were made from ATMs in areas other than the account holder's living area, and there is suspicion that the account was transferred and used fraudulently • In addition to attempts to deposit and withdraw cash, there are also withdrawals or remittances made after receiving unnatural transfers, and it is suspected that the account is being used in online and telephone fraud • There were transfers from an account that conducts transactions with multiple accounts that appear to be under fictitious names, making situations suspicious
Investigation results	It was discovered that the user of the account was committing fraud under the pretense of selling products, and the person was arrested.

(C) Cases of Theft/Computer Fraud (Online and Telephone Fraud)

Business type of the reporter	Deposit-taking institution/Cryptoassets exchange service provider
Reported account	Account in the name of Japanese

Reason for report	<Deposit-taking institution> • There is no rational explanation for the fact that the IP address when logging in is from abroad, or the browser language set to a foreign language, despite living in Japan • A typical transaction seen in fraudulent accounts, that is, a transfer from an individual and a full withdrawal on the same day <Cryptoassets exchange service provider> • There was a report from a financial institution that criminal proceeds had been transferred, and it is suspected that the proceeds are flowing into the accounts of cryptoassets exchange service providers • At the same time, there were movements that are often seen as preparations for fraudulent transactions, such as changes to email address and authentication methods
Investigation results	It was discovered that the account holder had received fraudulent remittance using a stolen cash card belonging to an elderly person's account, and the person was arrested.

(D) Cases of Violating the Cannabis Control Act[*1] (Possession for Profit) (Drug-related Offences)

Business type of the reporter	Deposit-taking institution/Credit card operator
Reported account	Account in the name of Japanese
Reason for report	<Deposit-taking institution> • Since the account was opened, there have been transactions with multiple individuals, and the activity is unnatural for an individual account • The account has received numerous transfers from individuals, and the funds were withdrawn at ATMs far from its registered address, and there is a suspicion of fraudulent use such as by loan sharks • A few days after the account was opened, a person who appears to be the same person as the account holder applied to open an account with a different pronunciation of the name • According to the camera footage installed at the ATM, it was found that a different person than the person in the identification image at the time of opening the account was operating the ATM, and transactions were made by multiple people using cash cards and smartphones in remote locations • Changed the name of the sender when transferring money <Credit card operator> • The credit card operator was unable to collect the service fee, so made multiple phone calls to remind the payment but with no answer. When they sent a reminder notice by mail, it was returned
Investigation results	It was discovered that the account holder was in possession of cannabis for the purpose of illicit trafficking, and the person was arrested.

(E) Cases of Violation of the Immigration Control and Refugee Recognition Act (False Application)

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of a former foreigner who had naturalized in Japan

[*1] Act No. 124 of 1948

Reason for report	• The account was opened for the purpose of paying living expenses. It aggregates remittances from individuals, including those whose accounts have been suspended and multiple foreigners with unknown relationship, and remits them to legal persons and individuals, and there is suspicion that it is an intermediary account • When the account holder was checked regarding the transfer from many individuals, it was discovered that the account was being used by a third party
Investigation results	It was discovered that the account holder and others had falsely applied for permission to extend their period of stay by pretending that they were married to Japanese nationals, and they were arrested.

(F) Cases of the Violation of the Act on Prevention of Transfer of Criminal Proceeds (Transfer for a Fee)

Business type of the reporter	Deposit-taking institution/Cryptoassets exchange service provider
Reported account	Account in the name of Japanese
Reason for report	<Deposit-taking institutions> • After receiving multiple transfers, almost the entire amount was transferred in a short period of time • After the email address has been changed, multiple transfers from third parties were received, and the funds were immediately transferred to another bank • Funds were transferred to a funds transfer service provider with the transfer requestor name changed to the name of a major e-commerce site • Repeatedly withdrawing funds from multiple individuals across Japan at ATMs in convenience stores located far from the registered address • Receiving transfers from an account that has been frozen as being used in online and telephone fraud • A withdrawal was made from an ATM on the same day after multiple individuals made transfers to the account that had not been used for a while after opening <Cryptoassets exchange service providers> • At the same time, there were movements that are often seen as preparations for fraudulent transactions, such as changes to email address and authentication methods
Investigation results	It was discovered that the account holder had opened multiple accounts for the purpose of transferring them, and had transferred the information, such as user IDs, necessary for using online banking to a third party for a fee, and the person was arrested.

(G) Cases of Violation of the Investment Act (Prohibition on the Receipt of Deposits)

Business type of the reporter	Deposit-taking institution
Reported account	1. Account in the name of Japanese 2. Account in the name of legal persons
Reason for report	• Suddenly, a large number of transfers and withdrawals were observed, with remittances and withdrawals being made to individuals with unknown relationships and a legal person represented by the account holder, but the details of the source of the funds, the purpose of receipt, and the usage are unknown. There is no consistency with the transaction purposes reported by the account holder, and the sudden increase in deposits and withdrawals is irrational [1] • After receiving funds of unknown origin from cryptoassets exchange service provider,

	the funds were withdrawn and transferred in a short period of time [1] • Using funds transferred from a specific legal person, remittances were made to multiple legal persons and individuals, and deposits and withdrawals have increased compared to the company's past transactions [2]
Investigation results	It was discovered that several people involved, including the account holder, were operating a business that accepted deposits of investment funds, and they were arrested.

(H) Cases of Violation of the Amusement Business Act (Operating in Prohibited Area)

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	• When applying to open an account, the explanation of the purpose and the occupation changed several times, which was suspicious • Frequently making payments using debit cards and flea market apps using funds deposited from ATMs. • The transactions are extremely frequent, and the source of the cash and details of the transaction background cannot be confirmed
Investigation results	It was discovered that the account holder and others were operating a store-based sex-related business in an area where such business is prohibited by law, and they were arrested.

(I) Cases of Uttering Counterfeit Official Documents with Signature or Seal

Business type of the reporter	Deposit-taking institution/Cryptoassets exchange service provider
Reported account	Account in the name of Japanese
Reason for report	<Deposit-taking institution> • An account holder reported receiving a cash card for an account opening that the person did not recognize <Cryptoassets exchange service provider> • Information was provided that funds were being transferred from the illegally accessed account to the financial institution account of a cryptoassets exchange service providers • Large amounts of funds were frequently deposited in a short period of time, exceeding the declared assets, and after the deposits were made, cryptoassets were purchased and repeatedly transferred to the same external address, resulting in large transfers of funds • Although the account was opened only recently, there were multiple accesses from different mobile operating systems, and the IP address location was in a remote location different from the registered address
Investigation results	It was discovered that the account user had fraudulently concluded a contract with a cryptoassets exchange service provider by sending image data of a forged driver's license, and the user was arrested.

(J) Cases of Violation of the Financial Instruments and Exchange Act[*1] (Unregistered Operation)

[*1] Act No. 25 of 1948

Business type of the reporter	Deposit-taking institution
Reported account	Accounts in the name of Japanese
Reason for report	• A transfer from a legal person suddenly occurred to an account with which there had been no transactions for about two years, and within a few days, withdrawals were made at an ATM • After a large cash deposit, the entire amount was transferred under a different name, which was a type of transaction that had never occurred before • Receiving an incoming remittance from a foreign legal person listed as an "unregistered financial instruments business operator" on the Financial Services Agency's website • Using inward remittances from abroad as funds, there were remittances to third parties with unknown relationships and over-the-counter withdrawal transactions, resulting in an increase in deposits and withdrawals compared to past transactions
Investigation results	It was discovered that several people involved, including the account holder (quasi-Boryokudan affiliate), were operating financial instruments business without registration, and they were arrested.

(K) Cases of Violation of the Trust Business Act[*1] (Unregistered Operation)

Business type of the reporter	Deposit-taking institution
Reported account	1. Account in the name of Japanese 2. Account in the name of legal persons
Reason for report	• There is suspicion of receiving fees related to the domestic sale of foreign funds that have not been approved by the Financial Services Agency [1] • The legal person that is the account holder supports the sale of unregistered insurance and investments in Japan, but is not a licensed business operator and is suspected of illegality [2] • Suddenly, a large amount of inward remittances was seen from a foreign legal person, but detailed information on the business status of the corporation was not available, and the background of the funds is unclear, making the sudden increase irrational [2] • A large amount of inward remittances is received from a foreign legal person and is sent to many individuals and legal persons, but the purpose of receipt is unknown and the transaction is irrational [2]
Investigation results	It was discovered that the representative of the legal person as an account holder was operating a trust contract agency business without registration, and the person was 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[*2] are as follows:

(A) Public Prosecutors Office

Case name	Fraud case, theft case

*1 Act No. 154 of 2004

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

Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese
Reason for report	• There are incoming transfers which seemingly has no reasonable relationship to the account holder's occupation • All the fund transfers are made by numerous but certain individuals on a frequent but irregular basis. Such funds are withdrawn or transferred to other individuals' account on the same day of the transfer, which always leaves the account with a small balance • Receiving sudden transfers from many individuals and then transferring or withdrawing the funds to many individuals

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

- Through illegal access to the server of financial institutions, offenders transfer fund from victims' account to financial accounts of cryptoassets exchange service providers. The offenders purchase cryptoassets with the illegally obtained money.
- Unlicensed moneylenders have their borrowers transfer the principal and usurious interest into moneylender's account opened under a third party's name.
- Offenders hide illicit profits in rented warehouse and coin lockers in trainstations.

(B) National Tax Agency

Case name	Cases of violation of Corporation Tax Act[*1]/Consumption Tax Act[*2]/Income Tax Act[*3]
Business type of the reporter	Deposit-taking institution
Reported account	Account under the name of Japanese and legal person
Reason for report	• Regarding an account under the name of a legal person, which receives large transfers and large amount of withdrawals of cash from the bank counter or ATMs, the employee who visited the deposit-taking institution was not aware of the purpose of the withdrawn funds or the business content of the legal person • A customer was making a large cash deposit at a bank counter, so the deposit-taking institution asked the customer what the source of the funds were.The customer then left without depositing the money.Later, a large amount of cash was deposited at an ATM • A certain account is frequently receiving large transfers from an unspecified number of individuals and legal persons, but the majority of the transfers from that certain account is being made to a specific individual

*1 Act No. 34 of 1965
*2 Act No. 108 of 1988
*3 Act No. Act No. 33 of 1965

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

- In 2023, the National Tax Agency accused cases involving the fraudulent receipt of consumption tax refunds (e.g. a case where fictitious taxable purchases and fictitious tax-free export sales were recorded by falsifying documents using the serial number of the same luxury watch and a copy of an illegally obtained passport, a case where fictitious tax-free export sales were recorded by using false passport information for duty-free products sold at a convenience store), failure to file tax returns (e.g. a case where income was earned through an affiliate marketing, but it was concealed by preparing false consulting contracts), and international cases (e.g. a case where income obtained by selling unlisted stocks in an illegal manner was disguised as income of a foreign legal person). It also accused cases having a high social ripple effect, including the following: a case where a professional enabler spread schemes of tax evasion by falsely reporting expenses, as tax savings and had it widely used by taxpayers; a case where a person whose business was to resell goods on the Internet and provide guidance on how to do so had been reporting fictitious expenses and excluding sales; a case where a factory equipment construction business operator, in a region where semiconductor manufacturing plants are actively being constructed, was reporting fictitious expenses; a case where a breeder recorded fictitious expenses in response to the increased demand for pets during the COVID-19 pandemic.From looking at the accused cases by their type of business, cases involving real estates and construction businesses is being ranked high in the number.
- Most of the illegal funds obtained through tax evasion is retained in the form of cash or bank deposits. In some cases, cash was concealed in bank safe-deposit box. In addition, there were cases where tax evaders have spent tens of millions of yen on the purchase of luxury vehicles, investments in securities, purchase of cryptoassets, gambling on horse racing and foreign casinos/online casinos, and entertainment and leisure expenses such as dining and drinking.

(C) Japan Customs

Case name	Cases of smuggling of illegal drugs
Business type of the reporter	Deposit-taking institution/Credit card operator
Reported account	Account in the name of Japanese/foreigner/legal person
Reason for report	• There was a transfer from abroad for a large amount of money for travel expenses, and the funds was transferred to a legal person with an unknown relationship • When transferring the money, the name was changed to that of a foreigner with an unknown relationship to the recipient • Cash transactions at ATMs continued in the account of a foreign student who had not applied or renewed the residence card upon expiration • Suspicious points were detected in the IP address, and access from multiple countries was confirmed • Frequent cash deposits at ATMs followed by repeated transfers to multiple legal persons, resulting in an increase in deposits and withdrawals compared to past transactions • Images captured by a camera installed at the ATM confirmed that the gender of the ATM user differed from that of the account holder, and that the cash card had been used by multiple persons • There is evidence that a person made withdrawals from ATMs on consecutive days, in large sums, and that the person tried to make withdrawals exceeding the payment limit

	• Transactions that exceed the declared assets have been made in a short period of time

[Recent Crime Cases and Trends Reported by Japan Customs]

- The smuggling of gold bullion 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 rising gold prices and a recovery in inbound tourism following the end of border control measures to prevent the spread of COVID-19, the number of cases is on the rise again, and future trends require close monitoring.
- In 2023, the number of detected cases of gold smuggling was 218 (approximately 24 times compared to the previous year), and the amount seized was approximately 268 kg (approximately twice as much as the previous year) with both the number of cases detected and the amount seized increasing compared to the previous year.
- One anticipated risk is that funds obtained through gold smuggling will be remitted to foreign countries via domestic financial institutions and used to purchase new gold bullion in foreign countries.

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

Case name	Cases of illicit trafficking of narcotics and methamphetamine
Business type of the reporter	Deposit-taking institutions/Financial instruments business operators/ Cryptoassets exchange service providers
Reported account	Accounts under the name of Japanese/foreigner/legal person
Reason for report	• Frequent small money transfers have been made at ATMs • Despite the account holder being a minor, multiple money transfers have been made by different individuals, followed by repeated immediate withdrawals during late-night at ATMs located in entertainment districts • Frequent round-number money transfers have been made by many different individuals, followed by immediate entire withdrawals at ATMs • In an ATM transaction using a smartphone, the smartphone's QR code was scanned in a foreign country, but the ATM used was located in Japan • A person who came up to bank counter to withdraw large amounts of cash acted suspiciously and gave a strange comments, saying that he would withdraw the money in several installments at multiple branches when asked about the reason for the transaction • The business purposes stated in the certificate of registered matters submitted when applying to open a legal person account were extremely diverse and appeared to have no relevance each other • Despite the account holder being an elderly person, during the identity verification call, the tone of the voice and the conversation suggested that someone else was impersonating the account holder • There was something odd about the format such as spaces, font, etc.-of the name on the driver's license submitted when applying to open a personal bank account

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

- For decades, a common modus operandi in the sale of illegal drugs such as narcotics, methamphetamine, and designated substances has involved the use of bank accounts under fictitious or third-party names. Customers, often recruited via social media, are instructed to transfer money to these accounts. To avoid identification, drug dealers typically advise customers not to use their real names when making transfers, but instead to use a fictitious name or a string of characters known only to the dealers.In recent years, however, a new trend has emerged; customers are now being instructed to use katakana spellings that phonetically match the names on the fictitious or third-party accounts. This is intended to evade detection by authorities. In some cases, dealers even seek to avoid bank transfers altogether.
- In this context, there have also been cases where the proceeds of drug-related crimes are disguised through fictitious transactions conducted on flea market apps. In one actual case, after receiving an order for illegal drugs from a customer, the drug dealer listed legal products-such as earphones, smartphones, clothing on a flea marketapp, despite not actually intending to sell these listed items. Once the purchased was made, the dealer shipped the illegal drugs instead. After the drugs were delivered, the customer was asked to confirm receipt through the app, enabling the dealer to receive payment or assets equivalent to the payment , such as points, thereby disguising the origin of the drug-related proceeds.
- As payment methods for drug trafficking, there have been cases where payments are made using online money transfer services, electronic gift certificates such as prepaid payment instruments, or QR code payments on smartphones. In particular, online money transfer services and payment methods using electronic gift certificates offer a high degree of anonymity, making it more difficult to identify the individuals sending payments for illegal drugs.
- Cryptoassets are sometimes used as a payment method when purchasing illegal drugs on foreign drug trafficking websites. In one case, a designer form of LSD considered a designated substance suspect object was shipped from Eastern European countries such as Bosnia and Herzegovina. Even after cryptoassets exchange used for past transactions had been frozen, a different exchange was utilized. The money were then transferred to a sales website via other overseas exchanges.

(E) Japan Coast Guard

Case name	Understanding of the actual circumstances of poaching organizations and their correlations with persons concerned
Business type of the reporter	Deposit-taking institution
Reported account	Account in the name of Japanese and foreigner
Reason for report	• Large amounts of cash transactions and remittance transactions have occurred • Frequent remittances were made in a short period of time, and almost the same amounts were deposited to and withdrawn from an account during a certain period • An account holder sent remittances to numerous individuals, including members or associates of Boryokudan

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

There are various forms of organized poaching, 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 theirs 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.

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:

Risk factors	High-risk transactions	
1. Transaction types	**Non-face-to-face transactions, cash transactions, cross-border transactions**	
2. Countries/regions	[Particularly high-risk] Countries/regions against which the implementation of countermeasures are requested by the FATF statements	**North Korea, Iran**
	Countries/regions against which the implementation of enhanced due diligence measures commensurate with the risks arising from the jurisdiction, as requested by the FATFstatements	**Myanmar**
3. Customer Attributes	Persons who intend to commit ML/TF	**"Boryokudans"** **International terrorists**
	Persons for whom it is difficult to conduct CDD	**Non-residents** **Foreign Politically Exposed Persons (Foreign PEPs)** **Legal persons (Legal persons without transparency of beneficial owners)**

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, driven by advancements in information and communication technologies, enhanced services by specified business operators focused on customer convenience, and efforts to prevent the spread of COVID-19.

For example, at deposit-taking financial institutions, it is possible to conduct financial transactions such as account opening, transfers, and cross-border remittances online, while financial instruments business operators 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. As a result, there are limitations on the information available about the counterparty

compared to face-to-face transactions.

When identity verification is conducted by mail or through eKYC[*1] using copies or images of identity verification documents, the accuracy of identity verification decreases because it is not possible to check for forgery or alteration based on the feel or texture of the documents. Direct verification of gender, appearance, and behavior is not possible, making it challenging to detect misrepresentation of personal details, impersonation of others, suspicious aspects of transactions, and illicit transfer of bank or transaction accounts. Consequently, the means to detect those planning criminal activities are limited, and it becomes easier for them to falsify their identity verification documents and personal identification details, impersonate others, and transfer bank or transaction accounts.

(B) Typologies

From 2021 through 2023, the main cases of non-face-to-face transactions being misused for ML include the following:

- 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.
- 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.
- The criminal proceeds, cash obtained through the thefts from ATMs, were deposited in multiple installments using ATMs into an account managed by the offender which had been opened using a forged relative's driver's license.
- 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.
- A criminal accessed the member website to reserve Shinkansen tickets on the Internet to obtain Shinkansen tickets through a non-face-to-face transaction by using illegally obtained credit card information.

(ii) Trends of STRs

In terms of reasons for submitting STRs regarding non-face-to-face transactions, the following reports focused on transactions suspected of impersonating fictitious people or other people, or of the use of a third party:

- 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, the registered email address is the same as that of an individual who had previously been reported as suspicious.

---

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

- Immediately after opening the account, the transfer limit was increased, 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 camera, it was found that a person other than the person on the identification document was using 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 transfers to 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 legal person accounts using ATMs.
- After multiple transfers were made from a legal person 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, 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

The Act on Prevention of Transfer of Criminal Proceeds and its Ordinance stipulate methods for verifying customer identities beyond direct receipt of identification documents. These methods include sending a copy of the identification document followed by forwarding transaction-related documents via registered mail or similar means, sending them via mail specifically addressed to the individual, and eKYC. Unlike face-to-face transactions, these methods do not allow for physical verification of the texture or quality of identification documents, making it difficult to detect forgeries. Therefore, specified business operators and those entrusted with identity verification tasks are accumulating knowledge on the characteristics of forged documents and utilizing AI for image analysis to detect forgery. They also check for suspicious details in reported information, such as addresses corresponding to vacant houses or phone numbers used for multiple account openings, thus taking measures to mitigate risks. Furthermore, for non-face-to-face transactions, the use of the Individual Number Card public personal authentication service (method of identity verification using a signature electronic certificate) makes it difficult to counterfeit, impersonate by third parties, or falsify data. Therefore, specified business operators are promoting the use of this method.

Discussions are underway, involving industry associations, regarding unifying non-face-to-face identity verification methods under the Act on Prevention of Transfer of Criminal Proceeds into the Individual Number Card public personal authentication in principle.

In addition, to detect unauthorized transactions by third parties after identity verification has been completed, specified business operators monitor transactions by verifying the rationality of IP addresses, login locations, and browser languages. They also consider reference cases in *the List of Reference Cases of Suspicious Transactions* published by the Financial Services Agency and characteristics of transfer accounts used in online and telephone fraud schemes, implementing risk mitigation measures such as submitting STRs and restricting account usage.

(iv) Assessment of Risks

As non-face-to-face transactions may hinder specified business operators from directly seeing customers and identification documents, the accuracy of customer identification can deteriorate. Therefore, compared with face-to-face transactions, non-face-to-face transactions make it easier for offenders to falsify customer identification data and pretend to be a fictitious or other person by falsifying identification documents. In addition, after identity verification has been completed, it is easier for a third party to conduct a transaction fraudulently than in face-to-face transactions.

Actually, there are cases where non-face-to-face transactions have been misused for ML, including a case where bank accounts opened by pretending to be other person or accounts illicitly transferred were misused. Considering this, it is recognized that non-face-to-face transactions present a high risk of being misused for ML/TF.

(2) Cash Transactions

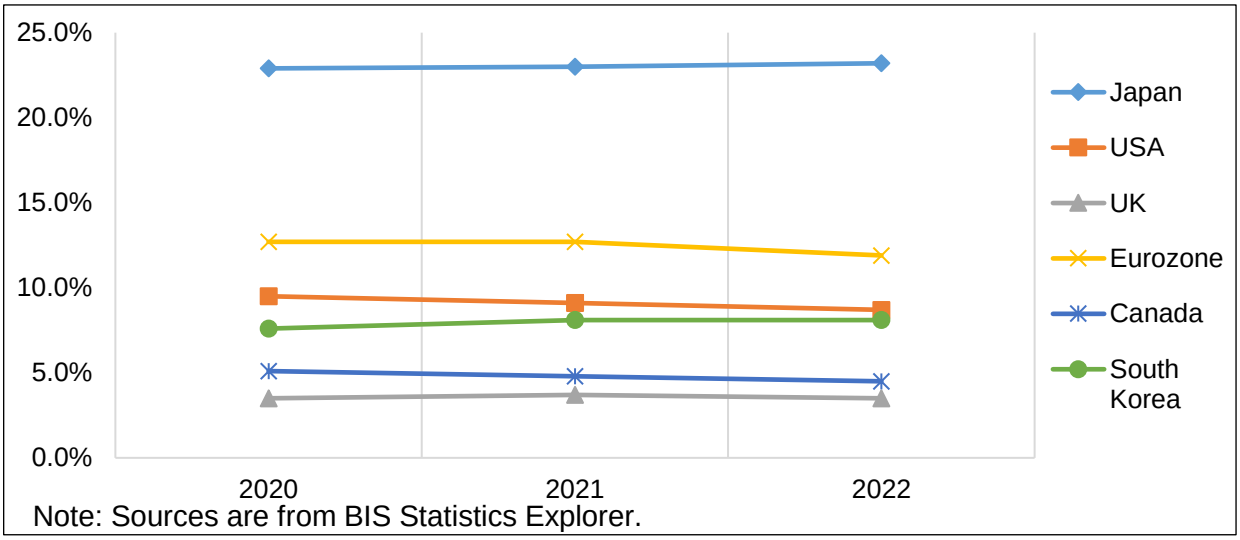
(i) Factors that Increase Risks

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

While a reasonable time is necessary for cash transactions because cash is physically transferred, cash transactions are highly anonymous, which is different from foreign/domestic exchange transactions where funds can be transferred to remote locations promptly. Cash transactions are unique in that the flow of funds is not easily traceable. Additionally, the vulnerabilities of products and services offered by specified business operators, combined with characteristics such as the liquidity of cash, can be misused for ML/TF.

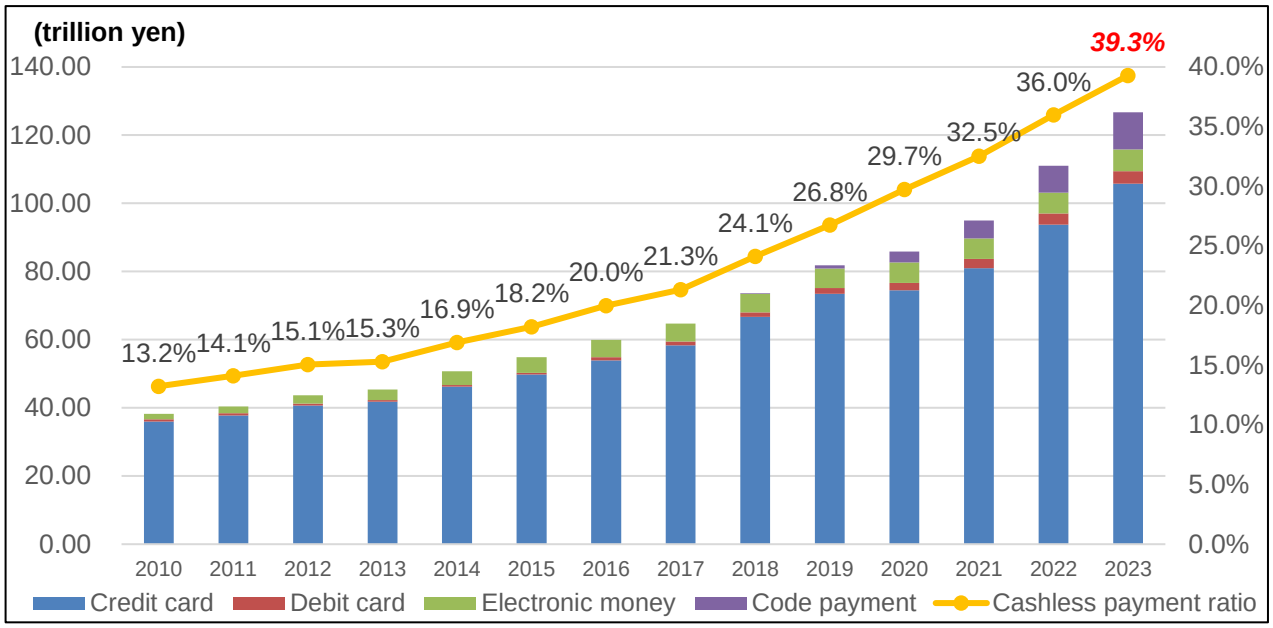
In Japan, cash is widely used as the primary means of payment, and the balance of cash in circulation is high compared to other countries (see Table 30). On the other hand, "Follow-up on the Growth Strategy" (Cabinet decision of June 21, 2019) set a goal of increasing the cashless payment ratio to around 40% by June 2025. As a result of efforts to promote this goal, the cashless payment ratio has been steadily increasing to 39.3% in 2023 (see Table 31).

Table 30: Ratio of Cash Distribution Balance for Different Countries in Nominal GDP



Note: Sources are from BIS Statistics Explorer.

Table 31: Trends in the Cashless Payment Ratio



(B) Typologies

The main cases where cash transactions were misused for ML between 2021 and 2023 are as follows:

- 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.
- An offender exchanged the cash, which was the proceeds of crime from armed robbery, for high-denomination bills at financial institutions and used ATMs to deposit the cash into an accounts in the relative's name.
- An offender withdrew some of the criminal proceeds obtained from fraud from a legal person account managed by the offender, and then entered into fixed-term deposits in the name of a relative at financial institutions and deposited the money into the account.
- An offender purchased a car with the cash, which was the proceeds of crime from armed robbery, and then sold it to a car dealer shortly thereafter, turning it into cash.
- An offender received criminal proceeds from online and telephone fraud, which were transferred to an account under fictitious or other party’s name, and refunded them in cash at an ATM.

(ii) Trends of STRs

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

- Consecutive cash transfers on the same day at an ATM (the transfer requester's name uses only the recipient's surname, and a different phone number is registered to prevent identification of the requester) were detected, and when the security camera images 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 increasing 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 remote from the registered address.
- After receiving a large amount of money from a legal person account, the money was withdrawn from an ATM every day just after midnight.

(iii) Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds and its Enforcement Order requires 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).

In addition, the Secondhand Goods Business Act (Act No. 108 of 1949) and the Pawnbroker Business Act (Act No. 158 of 1950) requires 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).

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 (ACT No.61 of 1954) 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 banknote detection dogs, to prevent the illicit export of cash and other items abroad.

Furthermore, the Japanese government intends to develop a cashless environment, as outlined in 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 make opaque cash assets visible, prevent opaque cash circulation, ultimately leading to the suppression of ML/TF associated with cash transactions.

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

- For cash deposits and withdrawals that exceed a certain level, a hearing sheet is issued at the teller, and STRs are submitted if necessary.
- 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.
- Requesting transfer to financial institution accounts instead of conducting cash transactions for trades involving jewelry and precious metals exceeding a certain amount.
- Monitoring suspicious cash withdrawals in ATM transactions and, if anomalies are detected, submitting STRs and/or conducting enhanced identity verification as defined in the Act on Prevention of Transfer of Criminal Proceeds, and restricting the use of accounts suspected of being used for crimes.

(iv) Assessment of Risks

In general, cash transactions have high liquidity and anonymity. Therefore, cash transactions may hinder the tracing of criminal proceeds. In fact, there have been many cases where money launderers misused cash

transactions by pretending to be other people. Considering this, it is recognized that cash transactions have carry a high risk of being misused for ML/TF.

(3) Cross-border Transactions

(i) Factors that Increase Risks

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

Japan has a highly advanced financial market and conducts a large number of transactions as one of the leading international financial markets around the world, occupying an important position in global economy.

Table 32: Statistics on Transactions with Foreign Countries

Item	Amount (yen)
Export value	100,873.8 billion
Import value	110,195.6 billion
Foreign exchange yen settlement amount	5,455.126 trillion
Annual cross-border transaction value of funds transfer service providers	1,673.298 billion

Note: The export value, import value and foreign exchange yen settlement amount are the results for 2023, and the annual cross-border transaction value of funds transfer service providers is the result for 2022.

In Japan, cross-border transactions are conducted on a daily basis, and these transactions have the following characteristics:

- Domestic legal and transaction systems vary from country to country.
- 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.

Cross-border transactions also have the following characteristics:

- Some foreign countries/regions allow the nominee system, under which legal persons' directors and shareholders can be registered in third-party names, and it is recognized that shell companies established in such countries/regions are being misused to conceal criminal proceeds. There is a high risk that the final remittance destination will become unclear if money is sent via such multiple highly anonymous legal person accounts.
- By disguising trade transactions, it is easy to pretend that the remittance is legitimate, and criminal proceeds could be transferred by paying more value than the genuine worth.
- In foreign exchange transactions, where payments are entrusted based on correspondent agreements[*1] between banks, money often passes through a series of remotely located intermediary banks, which may significantly hinder the tracing of criminal proceeds. 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

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

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.

Furthermore, in cross-border transactions, the following specific situations are recognized:

- Criminal groups committing online and telephone fraud are transferring criminal proceeds to foreign countries by transporting cash using cash couriers, transferring cryptoassets using foreign cryptoassets exchange service providers, and transferring funds via foreign accounts.
- Cross-border ML offences by international criminal organizations occurred in which proceeds from fraud committed abroad were transferred to financial institutions in Japan.

(B) Typologies

In cases where cross-border transactions were misused, not only offenders committing crimes in Japan, but also international crime organizations and foreigners, have been recognized to be involved.

The modus operandi include:

- To misuse financial institutions in and outside Japan (cross-border remittances);
- To disguise ML as legal trading (export or import of goods);
- To provide domestic and cross-border remittance and payment services without actually moving funds;
- To use cash couriers, and
- To misuse the transfer of cryptoassets.

Specific characteristics of modus operandi used in ML cases, in which offenders try to hide the true source of funds or facts about funds by disguising criminal proceeds from fraud committed in foreign countries as legitimate funds, include:

- A large amount of money, sometimes over 100 million yen, is remitted each time.
- The reasons for remittance given by the receiver and the remitter may be different.
- Almost all the remitted amount is withdrawn in cash.
- The remitters request reverse transactions later.

In ML cases or so-called underground banking*[1] cases disguised as legal trading, the following characteristics were found:

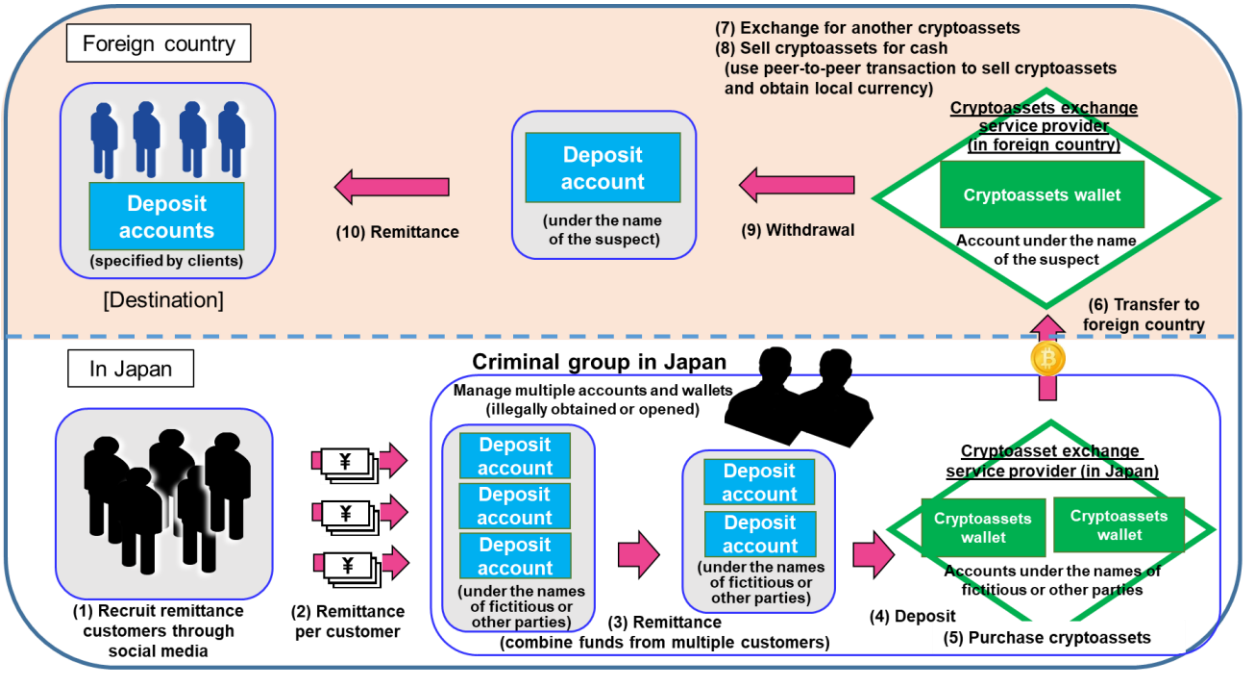
- When exporting a stolen vehicle, the export procedures are carried out as if it were a different vehicle, and the vehicle is exported to a foreign country under the guise of a genuine product.
- To export goods in high demand outside Japan (such as cars and heavy machinery) and convert them into cash at export destinations as a way to make cross-border remittances.
- The person operating the underground bank transferred the cash that had been transferred to a domestic account by the client to the account of a cryptoassets exchange service provider, and then purchased cryptoassets using an account under the name of fictitious or other party that had been obtained illegally. The person then transferred the cryptoassets to a cryptoassets wallet in a foreign country, sold

*[1] Underground banking refers to the act of a person without legal qualifications acting as an agent for cross-border remittances for a fee, and such acts are the violations of the Banking Act (Act No. 59 of 1981).

it through a peer-to-peer transaction to obtain foreign currency, and transferred it to a foreign bank account instructed by the client.

In this way, the forms of criminal proceeds change from cash to goods and back to cash again.

Table 33: Case of Underground Banking Using Cryptoassets

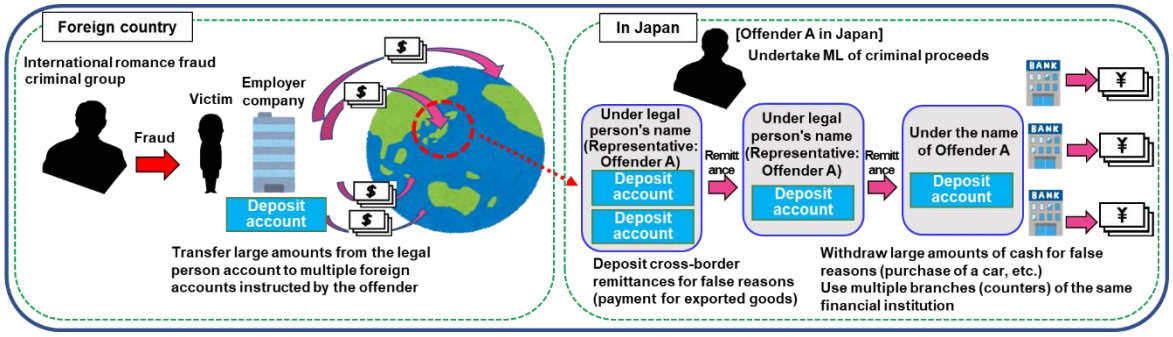


Regarding ML cases that have misused cross-border transactions between 2021 and 2023, the following incidents have been observed:

- An offender remitted money stolen by fraud (such as business email fraud (BEC)) in the US and Europe to an account opened at a bank in Japan. The Japanese account holder presented a forged invoice, claiming that the reason for the transfer was "office supplies," to withdraw the money by pretending to receive money remitted in a legal transaction.
- An offender had a victim transfer the money obtained through romance fraud via social media into an account under the name of fictitious or other party, and then gave false explanations for the reason for the transfer, such as "living expenses for a friend," and sent the money to a foreign bank account opened by the criminal group, disguising it as a legitimate cross-border transfer.
- When transferring fraudulent proceeds abroad, false reasons for the transfer were stated in the transfer reason section of related documents, and false invoices for the import of cocoa beans that were never actually imported were submitted as evidence, disguising the transfers as legitimate business transactions and sending funds to accounts in the perpetrator’s name opened at foreign banks.
- While the victim (a foreigner) of a fraud occurring abroad was being defrauded of money by repeatedly transferring money from an account in the name of his/her employer to numerous accounts in foreign countries, the offender who managed the deposit account in Japan received the money into a legal

person account managed by the offender, disguising it as an export advance payment for a legitimate trade transaction (export of computer equipment).

Table 34: ML Case Related to International Fraud



(C) Trends of STRs

The number of notifications of STRs related to cross-border remittances between 2021 and 2023 is as follows:

Table 35: Annual Number of Notifications of STRs Related to Cross-border Remittances

Ranking	Destination (origin) countries/regions	2021 (Number of cases)	2022 (Number of cases)	2023 (Number of cases)	Total (Number of cases)	Percentage (%)
1	China	11,685	11,286	13,428	36,399	28.1
2	Hong Kong	4,848	3,900	3,355	12,103	9.4
3	USA	4,150	3,866	3,178	11,194	8.7
4	Vietnam	1,772	5,714	2,165	9,651	7.5
5	South Korea	3,159	1,749	1,398	6,306	4.9
6	Philippines	1,755	2,146	2,354	6,255	4.8
7	Taiwan	2,124	1,975	1,616	5,715	4.4
8	Singapore	1,353	1,718	1,383	4,454	3.4
9	United Kingdom	1,684	1,633	1,029	4,346	3.4
10	United Arab Emirates	534	709	1,414	2,657	2.1
11	Russia	901	917	774	2,592	2.0
12	Thailand	780	716	784	2,280	1.8
13	Australia	548	696	604	1,848	1.4
14	Cambodia	400	637	733	1,770	1.4
15	Indonesia	485	599	625	1,709	1.3
16	Canada	495	444	327	1,266	1.0
17	Malaysia	494	388	378	1,260	1.0
18	Switzerland	372	293	201	866	0.7
19	Ireland	165	246	411	822	0.6
20	Myanmar	265	212	340	817	0.6
-	Others	5,382	4,744	4,951	15,077	11.7
-	Total	43,351	44,588	41,448	129,387	-

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 legal person account, submitted documents, such as a copy of the export license notice, shows that the transit point and export destination are countries/regions with a high ML/TF risk.
- 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 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 data provided by a foreign-exchange transaction operator whose country has similar legislation.
- 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

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

(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 it established, 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 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.

(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 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.
- 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.
- To check not only the purpose of the remittance but also the status of the recipient's use of the funds, and if there are any discrepancies, refuse the transaction and submit STRs.
- Monitoring cross-border remittance and trade finance transactions based on reference cases of suspicious transactions publicly disclosed by the Financial Services Agency and situations elevating the ML/TF risk in the interpretation notes of the FATF recommendations. Conducting in-depth investigations of transactions recognized as having a particularly high ML/TF risk and submitting STRs accordingly.

(iii) Assessment of Risks

In cross-border transactions, it is not easy to trace transferred funds compared to domestic transactions because of the difference in legal systems and transaction systems.

---

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

In fact, in some cases, ML has been conducted through cross-border transactions. Therefore, it is recognized that cross-border transactions pose a risk of being misused in ML/TF.

Furthermore, looking at recent trends in organized crime in Japan, there is a risk that criminal proceeds obtained by Anonymous and fluid criminal groups and Crime groups of foreigners in Japan may be transferred back to foreign countries.

Considering examples of situations that increase the risks of ML/TF as described 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:

- Transactions related to countries and regions where proper AML/CFT measures are not implemented.
- Cross-border remittances originated from large amounts of cash.
- 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] Diversification of payment methods in cross-border transactions and consideration of revising FATF Recommendation 16 on transparency of transfers

With the development of IT technology, payment methods are becoming more diverse. In cross-border transactions, in addition to bank transfers, it is also possible to transfer funds to foreign countries by utilizing the services of funds transfer service providers. It is also possible to transfer funds in effect by purchasing cash equivalents in foreign countries through card payments such as credit cards and debit cards. Furthermore, there are some methods, such as cryptoassets, that allow instant transfers across borders. There are various ways to transfer funds abroad, but those who attempt to commit ML/TF misuse the vulnerabilities of businesses and products/services, such as insufficient monitoring of fund transfers and transactions, and low transparency of transactions.

In October 2020, the Financial Stability Board (FSB) published the "G20 Roadmap for Enhancing Cross-border Payments." The main concern of the G20 and the FSB regarding cross-border payments is the pursuit of "faster, cheaper, more transparent and more inclusive" transfer services. The FATF also shares this concern and is working on revising FATF Recommendation 16 (hereinafter referred to as "Recommendation 16") to enhance cross-border payments from the perspective of improving AML/CFT measures.

Recommendation 16 aims to prevent criminals and terrorists from transferring funds through wire transfers, and to detect fraudulent transactions by enabling sending, relaying, and receiving financial institutions, as well as law enforcement agencies to access remittance information, such as information on the client, remitter, and recipient of cross-border payments. It was formulated as an FATF Special Recommendation, which was FATF's response to the September 11, 2001 terrorist attacks in the United States.

The purpose of the revisions to Recommendation 16 is to respond to various changes such as the diversification of payment methods and payment service providers, to ensure fair competition conditions, "same activity, same risk, same rules," which is the principle of the FATF standards, and to prevent the misuse of cross-border payment systems by criminals and terrorists while preventing loopholes in regulations related to ML/TF.

Revisions to Recommendation 16 is being considered primarily from the following perspectives:

(1) Clarifying the obligations of each actor in a series of cross-border payments in light of changes in payment business models

(2) Improving the content and quality of originator and beneficiary information in light of the transition to ISO 20022 wire transfer message format

(3) Reviewing the application of Recommendation 16 on card (credit, debit and prepaid) payments (transactions involving the purchase of cash equivalents above a certain threshold and cash withdrawals)

Ensuring a fair competitive environment and preventing loopholes in AML/CFT measures will contribute to improving the transparency of cross-border payments. However, there are challenges in achieving other policy objectives, such as increasing speed, reducing costs, and promoting financial inclusion, as well as addressing the impact on financial institutions and any side effects.

The FATF conducted a public consultation on proposed revisions to FATF Recommendation 16 during February - May 2024, and will continue to engage in dialogue with private sector entities while working to finalize the revision of Recommendation 16.

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, 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 to the FATF standards.

---

*[1] High-Risk Jurisdictions subject to a Call for Action

(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. They 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 data.

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 pose 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 recognized 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

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

Jurisdictions under Increased Monitoring for improving the AML/CFT measures. The FATF is calling on those countries/regions*[1] 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.

Moreover, even if there are no direct transactions with these countries, malicious and shrewd methods may be used to redirect funds through neighboring countries/regions, so thorough measures need to be implemented, including verification at the time of transactions.

[Topic] Changes in Countries/Regions for Which the FATF Requested Its Memberscountries/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 factors that increase the risk are based on the FATF Statement and will change accordingly. 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 over the last three years (2022 to 2024) regarding the designation of countries/regions for which the FATF requested its members countries/regions to apply countermeasures in the FATF statements and those designated under the FATF's monitoring process to improve their AML/CFT measures.

Note that the order of countries/regions is based on alphabetical order as of October 2024, with countries/regions publicly disclosed at the time of the FATF plenary meetings listed in Table 36 and countries/regions that have been disclosed in the past listed in Table 37.

Table 36: 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/ Period	2022			2023			2024		
	March	June	October	February	June	October	February	June	October
Iran	●	●	●	●	●	●	●	●	●
North Korea	●	●	●	●	●	●	●	●	●
Myanmar			◎	◎	◎	◎	◎	◎	◎

Table 37: 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/ Period	2022			2023			2024		
	March	June	October	February	June	October	February	June	October
Algeria									○
Angola									○
Bulgaria						○	○	○	○
Burkina Faso	○	○	○	○	○	○	○	○	○
Cameroon					○	○	○	○	○
Cote d'Ivoire									○
Croatia					○	○	○	○	○

*[1] jurisdictions under Increased Monitoring, as designated within the monitoring process.

DR Congo			○	○	○	○	○	○	○
Haiti	○	○	○	○	○	○	○	○	○
Kenya							○	○	○
Lebanese									○
Mali	○	○	○	○	○	○	○	○	○
Monaco								○	○
Mozambique			○	○	○	○	○	○	○
Namibia							○	○	○
Nigeria				○	○	○	○	○	○
Philippines	○	○	○	○	○	○	○	○	○
South Africa				○	○	○	○	○	○
South Sudan	○	○	○	○	○	○	○	○	○
Syria	○	○	○	○	○	○	○	○	○
Tanzania			○	○	○	○	○	○	○
Venezuela								○	○
Vietnam					○	○	○	○	○
Yemen	○	○	○	○	○	○	○	○	○
Albania	○	○	○	○	○				
Barbados	○	○	○	○	○	○			
Cambodia	○	○	○						
Cayman Islands	○	○	○	○	○				
Gibraltar		○	○	○	○	○			
Jamaica	○	○	○	○	○	○	○		
Jordan	○	○	○	○	○				
Senegal	○	○	○	○	○	○	○	○	
Turkey	○	○	○	○	○	○	○		
Uganda	○	○	○	○	○	○			
United Arab	○	○	○	○	○	○			
Nicaragua	○	○							
Malta	○								
Morocco	○	○	○						
Pakistan	○	○							
Panama	○	○	○	○	○				

* For the situation in each country, refer to the original text of the statement, "Jurisdictions under Increased Monitoring - 25 October 2024" (https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-october-2024.html)

[Countries and Regions with Suspended FATF Membership]

The FATF strongly condemned Russian Federation's war of aggression against Ukraine. During the FATF plenary meeting in February 2023, it was decided to suspend Russia's membership in the FATF. This decision was based on the conclusion that Russian Federation's actions unacceptably run counter to the core principles of the FATF, which aiming 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. Additionally, 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 surrounding Ukraine, Japan, aiming to contribute to the international efforts for peace and to maintain international peace and security, has taken measures under the FEFTA in line with those adopted by major countries. On February 26, 2022, the Japanese Cabinet agreed to implement asset freeze measures against certain banks in the Russian Federation and to prohibit transactions involving the issuance and circulation of new securities by the Russian Federation government and other governmental agencies. This also includes prohibitions on imports and exports between Japan and the self-proclaimed "Donetsk People's Republic" and

"Luhansk People's Republic," as well as export restrictions on items subject to international export control regimes to the 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.

3. Customer Attributes

The customer attributes that affect transaction risks were identified as follows, by referring to cleared cases in which Boryokudan gangsters committed ML and severe terrorism situations, 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"), as well as 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, etc.*[1]").

- Persons who intend to commit ML/TF:
  - (1) "Boryokudans"*[2]
  - (2) International terrorists (Islamic extremists, etc.)
- Persons for whom it is difficult to conduct CDD:
  - (3) Non-residents
  - (4) Foreign PEPs
  - (5) Legal persons (legal persons without transparency of beneficial owner)

Then, the above attributes were analyzed and evaluated from the perspective of factors that increase risks and measures to mitigate risks.

(1) "Boryokudans"

In Japan, “Boryokudans” conduct fundraising activities in disguise of legitimate business operations, or misusing business activities, as well as other various crimes to gain profit.

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

Boryokudan exist throughout Japan; their size and types of activities are many and various As of October 1, 2024, 25 groups are listed as designated Boryokudan under the Anti-Boryokudan Act.

At the end of 2023, the total number of Boryokudan gangsters was 20,400*[3] including 10,400 Boryokudan members and 10,000 associates*[4]. The grand total of these numbers started to decline in 2005, and as of the end of 2023, 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 measures to exclude Boryokudan from society. On the contrary, the number of those who

---

*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 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 In this NRA-FUR, "Boryokudans" refers to Boryokudan, Boryokudan-affiliated companies, "Sokaiya" racketeers, person(s) engaging in criminal activities under the pretext of social campaigns or political activities, and violent groups/individuals specializing in intellectual crimes, and Anonymous and fluid criminal groups.

*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.

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 smuggling of gold bullions. Moreover, Boryokudan commit crimes to obtain funds, disguising their activities as ordinary economic transactions by using Boryokudan-affiliated companies that Boryokudan substaintially 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. Criminal proceeds are funds to maintain and strengthen organizations by using them as operating capital to commit further crimes or to obtain weapons. Criminal proceeds may also be used to interfere with legal businesses.

Furthermore, Anonymous and fluid criminal groups are actively engaging in illegal fund-generating activities, such as online and telephone fraud, while they coexist and thrive alongside Boryokudan and others. They use the funds obtained through these activities as capital to expand into various industries, laborer including the adult entertainment industry, the entertainment sector (such as adult videos), and scouting. They also engage in ML and serve as a source of talent for online and telephone fraud.

Considering of the fact that the number of cleared cases of ML involving Boryokudan gangsters remains at the same level while the total number of Boryokudan gangsters is decreasing, it is considered that ML is still necessary for Boryokudan gangsters to obtain funds. In addition, Boryokudan and Anonymous and fluid criminal groups collude with each other to evade restrictions under the Anti-Boryokudan Act and the Organized Crime Exclusion Ordinances to shrewdly obtain funds.

(B) Typologies

---

*[1] he actual situation of Anonymous and fluid criminal groups is described in "Section 3. 1. (2) Anonymous and fluid criminal groups" in this NRA-FUR.

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

The main cases of ML involving Boryokudan gangsters from 2021 to 2023 are as follows:

- Boryokudan members received criminal proceeds from illegal gambling, prostitution or unlicensed adult-entertainment business in cash by calling the proceeds so-called "protection money," knowing that they were criminal proceeds.
- A Boryokudan member accepted goods purchased with criminal proceeds obtained from the unlicensed operation of an adult entertainment business as a gift, despite knowing the circumstances.
- A former Boryokudan member illegally accessed an online banking account and transferred money from a third party's account to an account under the name of fictitious or other party managed by the criminal, and then withdrew the cash.
- Boryokudan members withdrew cash transferred to accounts under the name of fictitious or other parties through online and telephone fraud. Then, they deposited it to their accounts, which were then further transferred to different accounts managed by others.
- Former Boryokudan gangsters used a portion of the proceeds obtained from fraud to establish companies, appointing relatives as directors with the intention of controlling the business, and using an unwitting judicial scrivener.
- A Boryokudan member made a debtor open an account and used it for receiving payments to a loan shark from other debtors or the names of family members.
- A former Boryokudan member instructed his accomplice to defraud a financial institution of money by obtaining a loan for fictious business and used bank accounts in the names of his acquittance and relative.
- A Boryokudan member organized an illegal gambling operation and then had players transfer their bets to an account in the name of a relative that the member managed.

The following facts have been revealed from the ML cases showing involvement of Boryokudan gangsters:

- They directly received criminal proceeds in cash; and
- They misused accounts of their acquaintances or relatives, delinquent persons or other Boryokudan gangsters for the purpose of disguising the ownership of criminal proceeds.

In this way, Boryokudan gangsters are engaged in ML using methods that make tracing of criminal proceeds difficult.

(ii) Trends of STRs

The number of STRs submitted from 2021 to 2023 was 1,821,396, including 177,228 STRs submitted for reasons related to Boryokudan, accounting for 9.7% 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.

The Financial Services Agency has formulated the Supervisory Guidelines and related measures for deposit-taking financial 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, “Boryokudans” conduct fundraising activities in disguise of legitimate business operations, or misusing business activities, as well as other various crimes to gain profitAs ML makes the source of proceeds obtained from criminal activities or fund-raising activities unclear, ML is indispensable to “Boryokudans”. Since "Boryokudans" engage in ML, transactions with "Boryokudans" 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, and Anonymous and fluid criminal groups are increasing their illegal fundraising activities, such as online and telephone fraud, while coexisting and prospering with Boryokudan. In light of this situation, it is necessary to examine CDD not only the direct counterparty to a transaction, but also to any substantive counterparties.

(2) International terrorists (Islamic extremists, etc.)

The threat of international terrorism remain high, with terrorist attacks occurring in various countries, including Europe and the U.S. Additionally, there are concern 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 on 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. The matters which should be paid attention to in terms of terrorist financing have increased and become more complicated. Thus, in this NRA-FUR, by referring to the FATF Recommendations, its Interpretive Notes, the FATF's reports, and measures under the Act on Prevention of Transfer of Criminal Proceeds, the following factors are discussed:

- ○ Threats (terrorist groups such as ISIL, AQ, and other Islamic extremists and their financiers)
- ○ Vulnerabilities (legal and illegal sources and methods of terrorist financing)

The NRA-FUR also discusses:

- ○ The impact of these factors on Japan

By comprehensively considering the above, ISIL, AQ and other Islamic extremists, foreign fighters, and individuals who have become extremists (hereinafter collectively called "Islamic extremists") were identified as customers who may become factors that affect risk.

(i) Factors that Increase Risks

(A) International Terrorism Situation

- ○ Islamic extremists

By March 2019, ISIL had lost all the territories it controlled in Iraq and Syria, but 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 has risen as the leader in August 2023. The following points have been pointed out about ISIL:

- ・ It has consistently called for acts of terrorism against Western and European 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 controlled territories and travel to their home countries or third countries to carry out terrorist attacks.
- ・ Some of those who remain in the former controlled territories are still active without being detained.
- ・ There is a possibility that further radicalization will occur in detention facilities or refugee camps.

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, 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.

---

*[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.

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 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. The Taliban have been considered to have close ties with AQ, and there are concerns that AQ's activities will intensify.

○ Threat of terrorism targeting Japan

No Japanese national or residency 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 approval. 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 united through extremism is affecting Japan. It is therefore possible that those who are affected by extremism of ISIL and AQ affiliated organizations could commit terrorism in Japan.

Table 38: Number of International Terrorism Cases

Item/year	2020	2021	2022
Number of cases	10,162	8,357	7,342
Number of deaths	29,326	23,712	21,943

Note: Based on the U.S. Department of State Country Reports on Terrorism

Table 39: Major Terrorism Cases in 2023

Date	Case
January 11	Suicide bombing terrorist incident near the Afghan Ministry of Foreign Affairs in
October 7 -	Clashes between Israel and Palestinian armed groups
October 13	Terrorist attack using a knife in Arras, France
October 16	Shooting terrorist attack in Brussels, Belgium
December 2	Terrorist attack using a knife in Paris, France
December 3	Terrorist bomb attack in Marawi, Philippines

Note: Excerpt from the National Police Agency's "The White Paper on Police 2024"

*[1] Abbreviation of Islamic State in Iraq and the Levant-Khorasan associated with ISIL.

(B) Characteristics

The characteristics of terrorist financing in light of international analysis related to the threat of and vulnerability to measures for terrorist financing are as follows:

- 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.
- 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.
- 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.

From the above, when filing STRs related to terrorist financing, it is necessary to pay attention to the following matters in addition to the points to be noted for ML.

- Customer attributes

Customer identification data, including names, aliases, and date of birth, concerning targeted persons of asset freezing under the FEFTA and the International Terrorist Asset-Freezing Act.

- Countries/regions

Whether remittance destinations and sources are countries/regions where terrorist groups are active or countries/regions in their neighborhoods.

Taking into account the following points indicated by the FATF, it should be noted that the risk of terrorist financing also exists in countries/regions other than those that are close to conflict areas, such as Iraq and Syria.

  - Technological advances, including social media and new payment methods, have introduced vulnerabilities in terms of terrorist financing.
  - In light of the cross-border nature of TF, a jurisdiction that faces a low terrorism risk may still face TF risks because funds or other assets may be collected or stored in it, or may be moved through.

- Transaction types
  - Whether the remittance destinations are groups or individuals whose status of activities is unclear, even if the remittance reason is a donation.
  - Whether the remitted money has been immediately withdrawn or transferred to another account.

(C) Domestic cases

Although there have been no cleared cases in Japan in relation to terrorist financing, the following cases are listed for reference:

- 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.

- 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.

(D) Cases in foreign countries

The cases in foreign countries are listed below. These cases contribute to the understanding of the actual situation of terrorist financing.

- Transfer of Funds from Social Security Account (Indonesia)

Between 2017 and 2018, Person A allegedly sent up to 60 million Indonesian Rupiah (equivalent to 4,000 US dollars) to siblings Person B and Person C, who were already involved with ISIL in Syria. It is claimed that Person A used Person B's identification card to withdraw cash from their social security insurance account and subsequently transferred the funds via an intermediary in Syria.

- Transfer of Terrorist Funds through Legitimate Money Transfer Service Providers (Australia)

In 2017, Australian university student A was convicted of sending funds abroad to support ISIL. Specifically, from July to September 2014, this individual sent 18,000 US dollars to Pakistan and Turkey, intending to assist those planning to travel from Pakistan to Syria to join ISIL as foreign fighters. The transferred funds are suspected to have been provided to Australian ISIL fighter B via an intermediary in Turkey, and it is alleged that these transactions utilized cross-border remittance services for transferring terrorist funds.

- Facilitation of Cryptoassets Usage for Terrorist Financing (United States)

In August 2015, an American, Person A, was sentenced to more than 11 years in prison and lifetime surveillance for supporting ISIL. Person A admitted to sharing methods on social media for concealing ISIL funding using Bitcoin and offering assistance to ISIL sympathizers planning to travel to Syria. Person A provided advice to ISIL and its supporters, including methods to facilitate anonymous Bitcoin transactions.

For instance, Person A admitted to supporting the travel of a US-resident minor with intentions of joining ISIL for combat purposes to Syria in January of the same year. 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. Notably, 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, including links to his article titled Bitcoin for Sadaqat al-jihad (Bitcoin and the charity of Jihad), which explained Bitcoin and its system and introduced new tools for anonymizing Bitcoin users, all shared on social media.

---

*[1] The Japanese Red Army has been responsible for numerous international terrorist incidents in the past, and currently, 7 fugitive members are wanted internationally. Efforts are underway to apprehend the fugitive members and clarify the organization's activities.

- Travel to Conflict-affected Area with Loan from Banks (Malaysia)

In 2014, 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 dollars, 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 US dollars). 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.

(ii) Trends of STRs

Specified business operators have actively submitted STRs regarding transactions suspected to be related to terrorism financing. The characteristics of STRs are as follows:

- The name of a customer is similar to the name of a person who was reported as a person subject to asset freezing or a person involved in terrorism.
- Specified business operators submit STRs because terrorist financing is suspected based on the customer attributes and transaction types.
- Looking at the types of transactions for which STRs have been submitted, transactions with foreign countries occupy a large share, and many of them are countries and regions in Asia and the Middle East.
- Some specified business operators looked at the customer attributes and submitted STRs on transactions in which cash was withdrawn with a debit card multiple times, resulting in the withdrawal of a large amount of cash in the above countries and regions.

(iii) Measures to Mitigate Risks

(A) 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 International Convention for the Suppression of the Financing of Terrorism and other measures to prevent terrorist financing.
  - 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."

(Article 1)

- 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. (Articles 2 to 5. Amendments made in response to the FATF Recommendations Act have 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 May 10, 2024, 420 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 May 10, 2024, the names of 420 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.

(B) 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 measures to strengthen efforts to counter terrorist financing, including 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
  - 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.

(iv) Assessment of Risks

Japan has been implementing the abovementioned measures. As a result, 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 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 particular, it is acknowledged that there is a high risk of terrorist financing when conducting transactions with people who are considered to be 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.

---

*[1] Terrorist Financing Risk Assessment Guidance (July 2019)

[Topic] Risk of Abuse of Nonprofit Organizations*[1] for TF

The FATF, in Recommendation 8, also calls its member countries to prevent nonprofit organizations from being abused by terrorists. In this topic, the risk of terrorist financing for nonprofit organizations, which is a premise of the risk-based approach, is analyzed and evaluated.

1. Characteristics

Nonprofit organizations in Japan engage in various social contribution activities and are a collective term for organizations that do not aim to distribute profits to their members. Individual laws regulate their establishment and management.

According to the FATF Recommendations and its Interpretive Notes, not all nonprofit organizations are at high risk. Since the risk level varies depending on the nature and scope of activities, the response must depend on the threat and vulnerability of individual organizations*[2]. In addition, the following are listed as vulnerabilities of nonprofit organizations to terrorist financing:

- ○ Nonprofit organizations, having gained societal trust, can access various funding sources and often handle significant amounts of cash.
- ○ Some operate in or near areas affected by terrorist acts, providing financial transaction frameworks.
- ○ There are instances where the entities raising funds for activities differ from those disbursing them, leading to a lack of transparency in fund usage.

Furthermore, considering examples in foreign countries, potential threats include:

- ○ Terrorist organizations and their associates may establish nonprofit organizations under the guise of charitable activities, using the funds raised to provide support for terrorists and for their families.
- ○ Legitimate nonprofit organizations can be infiltrated by terrorist associates, who misuse financial transactions to funnel money to terrorists, particularly in conflict zones.
- ○ Funds from legitimate nonprofit activities may be channeled to overseas nonprofits linked to terrorist groups, becoming sources of terrorist financing.

The FATF Recommendations highlight methods of misusing nonprofit organizations: a terrorist organization pretends to be a legitimate group; a legitimate group is used as a pipeline for terrorist financing; or legitimate funds are diverted into terrorist organizations. Furthermore, United Nations Security Council Resolution 2462, which was adopted in March 2019, expressed serious concern that terrorists may procure funds by abusing lawful companies or nonprofit organizations and transfer funds through lawful companies or nonprofit organizations, by taking advantage of new financial technology such as cryptoassets.

2. Nonprofit Organizations in Japan

Each competent administrative authority supervising nonprofit organizations in Japan conducts risk assessments and uses a risk-based approach to monitor nonprofit organizations. The main results of the risk assessment of nonprofit organizations conducted by the competent administrative authorities are as follows:

(1) Corporations Engaging in Specified Non-profit Activities (CESNAs) <Cabinet Office>

(i) Characteristics

A specified nonprofit corporation (hereafter referred to as “CESNAs”) is an entity primarily focused on conducting specified nonprofit activities as defined in the Act on Promotion of Specified Nonprofit Activities (Act

---

*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 or fraternal purposes, or for the carrying out of other types of good works,” the Strategic Policy 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 of terrorist financing must not hinder or prevent them from carrying out legitimate charitable activities.

No. 7 of 1998, hereafter referred to as the "APSNPA"). "Specified nonprofit activities" are those falling under the 20 categories of activities listed in APSNPA, aiming to contribute to the welfare of a broad and unspecified number of people. The areas of activity for NPO corporations include, for example, activities aimed at promoting health, medical care, or welfare, advocating for human rights or peace, and engaging in international cooperation. When establishing a CESNA, the required application to the relevant authority includes the articles of incorporation detailing the types of specified nonprofit activities and related businesses, lists of officers and at least ten members with their names and addresses, along with a statement of purpose and a business plan. This application undergoes an examination, and certification is granted upon approval. As of the end of July 2024, there are 49,714 CESNAs.

The vulnerabilities of CESNAs to exploitation for terrorist financing include:

○ Operating in or near regions where terrorist acts occur.

Some CESNAs operate in areas prone to terrorism and conflicts, including their vicinity, for humanitarian reasons. However, operating in these areas often complicates the effective management of organizational resources. Additionally, the operational areas of these corporations may overlap with terrorist active zones, and the people they assist could coincide with those approached by terrorists. These circumstances encourage the misuse of CESNAs for terrorist financing.

○ Having access to substantial sources of funds and the ability to transfer funds abroad or carry cash out of the country.

Some CESNAs have access to significant sources of funds and transfer these funds abroad to support conflict areas or disaster-affected regions. During these operations, cash is often intensively managed, and sometimes cash itself is physically transported. The use of highly anonymous methods for sending funds abroad and carrying cash, in particular, complicates the tracking of terrorists and their supporters, thereby encouraging the misuse of CESNAs.

○ Collaboration with partners and the utilization of volunteers in foreign countries.

When CESNAs expand their activities abroad, they frequently collaborate with local partners, and many volunteers participate in their operations. Such collaboration with partners abroad and the utilization of volunteers can make it difficult to scrutinize the identities of those involved and may invite the involvement of terrorist organizations and their supporters.

○ The presence of dormant or unclear activities.

Some CESNAs are in a so-called "dormant state," and others have unclear activity records, with business reports indicating "no activity performance" or "no expenditure during the fiscal year." Such corporations can be susceptible to exploitation by terrorist organizations and their supporters.

(ii) Measures to Mitigate Risks

Regarding the risk of terrorist financing by CESNAs, APSNPA provides general supervisory authority for competent authorities to collect reports with penalties, conduct on-site inspections, issue improvement orders and revoke certification of establishment. It is considered that this supervisory authority, together with other major actions to mitigate TF risks under laws and regulations of Japan, mitigates the risk of CESNAs being abused for TF.

In addition, in October 2023, the Cabinet Office updated the "Guidance for Countermeasures against Terrorist Financing by CESNAs" 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, helping to mitigate the risk of TF for CESNAs.

Furthermore, in October 2023, the monitoring based on a risk-based approach was started, in which the competent authorities approach CESNAs individually after confirming the activities of CESNAs and their

countries/regions and narrowing down the target CESNAs. This monitoring is highly effective, based on detailed implementation procedures, and is expected to further mitigate the TF risk for CESNAs.

(2) Public Interest Corporation <Cabinet Office>

(i) Characteristics

Public interest corporations, established for conducting public interest projects as defined by the Act on Authorization of Public Interest Incorporated Associations and Public Interest Incorporated Foundations (Act No. 49 of 2006), include activities in academia, arts, charity, etc., that contribute to the welfare of a broad and unspecified populace. To become a public interest corporation, a general incorporated association or foundation must apply for public interest certification, undergo review and recommendation by a third-party organization, and receive certification from the administrative agency. As of September 1, 2024, there are 9,730 public-interest corporations.

The vulnerabilities of public interest corporations to terrorist financing are as follows:

○ Engaging in activities in areas where terrorist acts are taking place or in their vicinity.

While only a small number of public interest corporations operate in regions exposed to the threat of terrorism and its surroundings, those entities tend to face relatively higher risks.

○ Engaging in outsourcing or grant assistance to carry out operations abroad.

Public interest corporations use various methods for executing their operations. Not only do they conduct activities directly, but they also engage indirectly through outsourcing or grant assistance. When different entities handle the fundraising and disbursement of funds, especially in foreign operations, this separation can lead to opaqueness in fund utilization, making it difficult to confirm fund management and intended use.

○ Handling substantial amounts of funds, including transfers to foreign countries and cash handling in foreign countries.

Some public interest corporations handle significant amounts of funds, thus having potential vulnerabilities that terrorist organizations could exploit. The risk of exploitation increases when these corporations transfer funds abroad or manage cash in foreign countries.

(ii) Measures to Mitigate Risks

Public interest corporations are considered to be able to mitigate TF risks to a certain extent through the appropriate application of statutory measures by administrative authorities and risk recognition and countermeasures by each public interest corporation. In particular, in order to prevent public interest corporations from becoming involved in TF, it is important for each public interest corporation to recognize the TF risks and take appropriate measures in accordance with the risks it faces. The "Countermeasures Against Terrorist Financing by Public Benefit Corporations" (published by the Cabinet Office in June 2022) encourages public interest corporations to take specific measures commensurate with the risks they face, and this is considered to mitigate the risk of them being misused for TF.

(3) Social Welfare Corporation <Ministry of Health, Labour and Welfare>

(i) Characteristics

Social Welfare Corporations are legal entities established with the purpose of conducting social welfare activities as stipulated in 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 various documents and obtain approval from the relevant authorities. As of March 31, 2023, there are 21,113 social welfare corporations.

Furthermore, social welfare corporations are established with the objective of conducting social welfare activities, such as operating elderly care homes. Hence, their activities abroad are limited. In analyzing the factors and perspectives by which social welfare corporations conducting activities abroad could be exploited for terrorist

financing, we identified factors related to (1) Products and services, (2) Transaction methods, (3) Countries and regions, and (4) Customer attributes. While cash transactions and dealings with foreign entities are allowed, most of their transaction partners are considered equivalent to public institutions or businesses that have conducted attribute verification.

(ii) Measures to Mitigate Risks

When social welfare corporations conduct activities abroad, the intention to conduct overseas activities in the articles of incorporation must be included, and approval must be obtained from the relevant authority. Additionally, separate financial statements are prepared to distinguish domestic operations from activities abroad. Furthermore, in the annual status report submitted, specific provisions mandate the clear disclosure of activities abroad, including their nature and the implementing country, and this information is considered in the appropriate monitoring by the relevant authority. As a result, it is believed that the risk of TF has been reduced.

(4) Medical Corporation <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 requires approval from the governor of a prefecture to establish hospitals, clinics, and similar facilities within Japan. As of March 31, 2024, there are 58,902 medical corporations. As of July 1, 2024, 10 medical corporations are engaged in activities abroad. The activities of medical corporations abroad are limited to the operation of foreign medical institutions and the provision of medical technology and education to healthcare professionals abroad. These activities require approval from the relevant authorities.

Factors and perspectives on the misuse of terrorist financing by medical corporations engaged in activities abroad were analyzed using the same criteria as those for social welfare corporations. It has been confirmed that cash transactions and dealings with foreign entities are allowed. However, the services provided are limited to medical-related activities, and the customer attributes are restricted to individual patients or healthcare professionals. Additionally, the relevant authorities regularly monitors the activities of medical corporations through approval for commencing activities, advance notification for investments, and submission of business reports.

(ii) Measures to Mitigate Risks

For medical corporations, in addition to the major legislative measures in Japan that contribute to reducing the risk of terrorist financing, supervision is conducted based on the general supervisory authorities stipulated in the Medical Care Act. Specifically, when medical corporations develop new businesses, including activities abroad, they are obligated to amend their articles of incorporation and obtain approval from the relevant authority for such changes. 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, it is stipulated that the corporation should be dissolved. Also, by requiring medical corporations to report their annual activities, the relevant authorities conduct supervision, which is believed to reduce the risk of terrorist financing.

(5) School Corporation <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 based on the provisions of the Private School Act (Act No. 270 of 1949), which stipulates the purpose, name, and other specified matters in the act of donation. As of May 1, 2023, there are 7,722 school corporations.

Furthermore, school corporations are established with the purpose of establishing and operating private schools and their activities abroad are limited. To analyze the factors and perspectives on the misuse of school corporations by terrorist financing engaged in activities abroad, similar criteria to those for social welfare corporations were considered. It was found that while dealings with foreign entities are permitted, transactions are

limited to certified entities or individuals with confirmed attributes, mainly involving educational and research activities, accounting for 98% of their operations abroad as of 2022.

(ii) Measures to Mitigate Risks

Regarding school corporations' activities, including ventures abroad, they are obligated to create and disclose financial documents and business reports annually. School corporations receiving subsidies from the relevant authorities are required to submit financial documents and business reports to those authorities. Additionally, when engaging in activities aimed at generating revenue beyond educational and research activities, school corporations must include such activities in their defined donation practices and obtain approval from the relevant authorities. This approach contributes to reducing the risk of terrorist financing.

(6) Religious Corporations <Ministry of Education, Culture, Sports, Science and Technology>

(i) Characteristics

Religious corporations are formed when religious groups obtain legal entity status through approval from the relevant authorities. To establish such entities, they must adhere to the regulations stipulated by the Religious Corporations Act (Act No. 126 of 1951), including specifying their objectives, name, and other required details, for which they must obtain approval from the relevant authorities. As of December 31, 2022, there were 179,339 religious corporations in existence, with approximately 99% of them, or 178,144, falling under the jurisdiction of prefectural governors in a single prefecture. Moreover, around 72% of religious corporations reported annual incomes below 5 million yen*[1].

In addition, regarding 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 acquired by third parties, leading to issues such as terrorist financing, tax evasion, and misuse for profit-oriented activities. As of December 31, 2023, 4,431 corporations have been identified as inactive religious corporations.

(ii) 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 taking measures to ensure that all religious corporations fulfill their obligation to submit copies of financial documents kept in the office, including rigorous enforcement of reminders and proper implementation of penalty measures. Furthermore, the Agency is actively promoting measures to address inactive religious corporations. In March 2023, a notification was issued to all prefectures to ensure the thorough implementation of these measures, followed by a meeting of department heads the following month to provide direct explanations.

Specifically, the Agency is emphasizing the need for prefectures to rigorously enforce reminders for religious corporations that have not submitted their office's required documents. For corporations where submission is not expected in the end, procedures for imposing penalties are to be carried out. Additionally, clear criteria have been established for identifying inactive religious corporations. For instance, corporations with unknown whereabouts of their representative officers and those that repeatedly fail to submit copies of financial documents kept in the office are categorized as inactive religious corporations.

Furthermore, since fiscal year 2023, the Agency for Cultural Affairs has been providing support to prefectures in their efforts to implement measures against inactive religious corporations through the project to promote measures against inactive religious corporations, and has been taking measures to mitigate the risk, such as

---

*[1] Survey report on activities conducted by religious corporations (as of October 1, 2021).

mentioning and raising awareness of the risk of inactive religious corporations being misused by criminal organizations at prefectural training sessions for religious corporation administrative officials.

(7) Other Organizations

(i) Characteristics

"Good works" as defined by the FATF can be conducted by general incorporated associations or general foundations, or even by voluntary organizations without juridical personality. The Ministry of Foreign Affairs of Japan and 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 organization size (revenue size) is 40 million yen.

(ii) Measures to Mitigate Risks

General incorporated associations, general incorporated foundations, voluntary organizations, and other entities that meet the definition of nonprofit organizations under the FATF but have not yet been certified due to differences in their legal personalities, are limited in size and activities, and are subject to regulations imposed on FIs under the Act on Prevention of Transfer of Criminal Proceeds and the FEFTA when transferring funds. Furthermore, general incorporated associations and general incorporated foundations, which are not subject to certification or accreditation, 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) (with a fine for failure to register). Thereby the law enforcement authorities have access to the registered information on those legal persons and risk mitigation measures are in place. Therefore, the risk of these entities being misused for TF is relatively low compared to nonprofit legal entities under the six laws.

3. Assessment of Risks

In Japan, the risk of being exploited for TF is high in the following cases, and considering Japan's position and role as an international financial market, it is also necessary to consider the guidance provided by international organizations on the transfer of terrorist funds through nonprofit organizations in financial transactions:

- ○ 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.

It should be noted that there have been no cases of nonprofit organizations being prosecuted for being exploited for terrorist financing in Japan and limited number of nonprofit organizations conduct activities abroad. Therefore, it is considered that they are at a low risk of abuse.

In the future, taking into account the increasing international concerns, it is essential to periodically reassess the risk associated with nonprofit organizations and carry out monitoring by the relevant government agencies based on the assessed risk levels. Furthermore, it is necessary to continue outreach efforts regarding the risk of terrorist financing and its mitigation measures to ensure the integrity of the activities of nonprofit organizations operating in high-risk areas, thus preventing them from being used for terrorist financing.

*[1] Ministry of Foreign Affairs and Japan NGO Center for International Cooperation, "NGO Databook 2021: Statistics on Japan's NGOs" (February 2022)

(3) 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 identity verification and verification of assets and income, for non-residents are limited compared to those for residents. 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 determine whether or not identification documents are authentic because the identification documents or supplementary documents used to verify the identity of non-residents are issued by foreign governments. Therefore, there is a higher risk of specified business operators conducting transactions with customers who are lying about their identity 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.

(iii) Assessment of Risks

In the case of transactions with non-resident customers, specified business operators 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.

(4) 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 data 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 Unfair Competition Prevention Act (Act No. 47 of 1993) was amended, and prohibitions on providing illicit profits to foreign public officials were introduced in 1998.

Although specific cases of ML/TF related to foreign PEPs have not been reported in Japan thus far, there have been some cases of violating the Unfair Competition Prevention Act (illegal provision of benefits for foreign public servants) in recent years. The following cases are examples of the violation of the Unfair Competition Prevention Act:

- 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 handed 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 abroad.
- A former director of a Japanese company handed cash to a foreign public official as a reward for acknowledging the company's breach of conditions in connection with the construction business of a thermal power plant ordered in a foreign country.
- A former president of a Japanese company gave 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 as a gift for issuing the documents needed to apply for statuses of residence and to submit notifications of marriage.

(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 data, 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.

(iii) Assessment of Risks

Foreign PEPs have positions and influence that can be misused for ML/TF. Grasp of their identification data is limited, and efforts to introduce anti-corruption measures vary from jurisdiction to jurisdiction. Depending on the situation, it is recognized that transactions with foreign PEPs present a high risk in terms of ML/TF.

(5) 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 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 vary depending on the type. (See Tables 40, 41, and 42.)

Table 40: Number of Corporations by Major Corporate Type in Japan

Year / Category	2020	2021	2022
Stock company	2,583,472	2,612,677	2,691,378
General partnership companies	3,352	3,325	3,068
Limited partnership companies	12,969	12,482	12,290
Limited liability companies	134,142	160,132	184,719
Others	70,436	75,770	22,798
Total	2,804,371	2,864,386	2,914,253

Note 1: The company sample survey of the National Tax Agency.
2: The number of corporations is the total number of non-consolidated corporations and consolidated 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 41: Number of Registered Establishments by Each Major Corporate Type

Year / Category	2021	2022	2023
Stock company	95,222	92,371	100,669
General partnership companies	16	20	15
Limited partnership companies	33	30	17
Limited liability companies	37,072	37,127	40,751
Total	132,343	129,548	141,452

Note: The statistics of the

Table 42: 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 ML/TF that arise from these characteristics.

<table>
<tr><th colspan="2">Characteristics unique to legal persons</th></tr>
<tr><td>Structure</td><td>○ 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.</td></tr>
<tr><td>Transactions</td><td>○ 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.</td></tr>
<tr><td>Corporation type</td><td>○ 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.</td></tr>
<tr><td>Other</td><td>○ 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.</td></tr>
<tr><th colspan="2">Vulnerabilities regarding ML/TF</th></tr>
<tr><td colspan="2">○ 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.</td></tr>
</table>

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

Regarding the ML offences apprehended from 2021 to 2023, the following table shows the number of cases where shell or opaque corporations were misused, and the number of such misused legal persons.

Table 43: Number of Cases Where Shell or Opaque Corporations Were Misused/Number of Misused Legal Persons

	2021	2022	2023
Number of cases	16	6	15
Total by type of legal person	23	11	23
Stock companies (including special limited liability company)	16	9	19
Limited liability companies	6	1	4
General partnership companies	0	0	0
Limited partnership companies	0	0	0
Other	1	1	0

The following cases are common examples of misusing non-transparent legal persons for ML from 2021 through 2023:

- Offenders purchased a shell company, had the fraudulent funds transferred to an account in the name of that company, and then transferred the funds to an account in the name of another company, then used the account in the name of another company to purchase cryptoassets.
- Unregistered money lenders purchased inactive company, or had others establish company on the condition that they would reduce their debts, and then had them transfer the principal and interest equivalents of loans they had made at illegal interest rates to an account in the name of the company.
- Offenders purchased accounts in the names of inactive company, concealed the fact that the company was inactive from financial institutions, and had financial institutions transfer criminal proceeds via cross-border remittances, pretending that the proceeds were legitimate business income in line with their business purposes, and then received repayments.
- Offenders disguised the criminal proceeds obtained through fictitious billing and other inflated charges as legitimate business profits by issuing fictitious invoices, and had the proceeds transferred via a so-called conduit company to an account held by an inactive company posing as a subcontractor.
- When establishing a company, an offender used the criminal proceeds to pay the full amount of the contributions for the issued shares, thereby acquiring the status of founder of the company, and appointed an acquaintance as representative to take control of the business management.

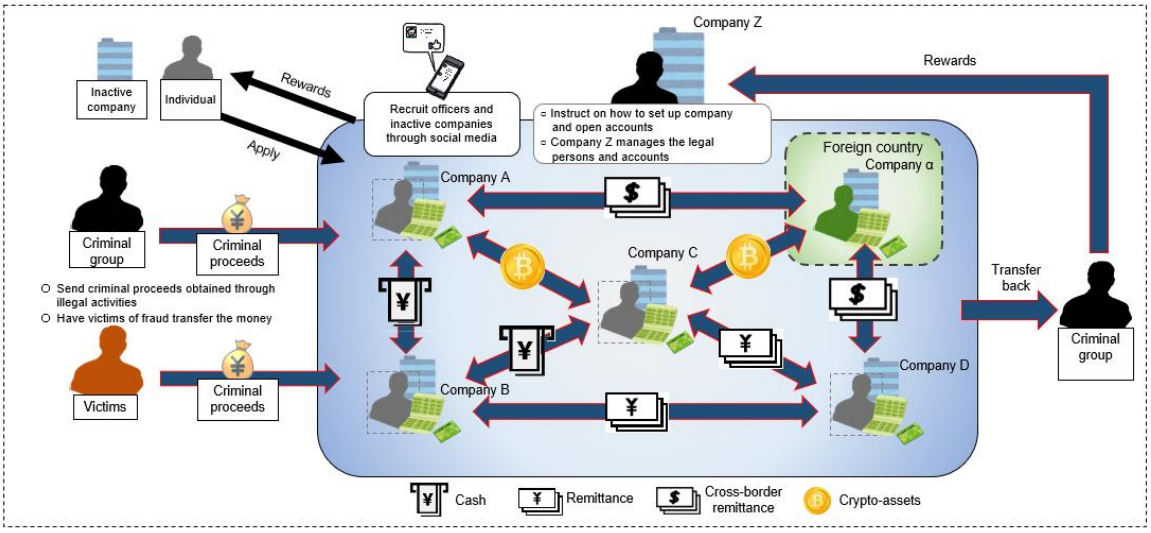
Looking at domestic cleared ML cases misusing legal persons, the following circumstances were observed:

Characteristics of misused companies
○ Establish a shell company. ○ Acquire an existing company owned by a third party. ○ Appoint a third party as the representative. ○ Request and use a company owned by a third party operating a legitimate business to send and receive criminal proceeds.
Registration of misused companies
○ Established with a small amount of initial capital (tens of thousands to hundreds of thousands of yen). ○ Frequently change locations or officers in the register. ○ Many business purposes are registered, with little relevance between them. ○ The business purpose is changed to something that makes it easier to explain the disguise of criminal proceeds (e.g. a type of business providing services that do not handle physical goods).
Status of establishment
○ Compared to stock companies, limited liability companies tended to be misused sooner after their establishment, with some being misused within a few months of their establishment.
Predicate offences
○ More than half of the offences are fraud. ○ Other offences include embezzlement, violation of the Amusement Business Act, violation of the Investment Act/Money Lending Business Act, habitual gambling, etc.

These situations show that shell or opaque corporations are being misused in crimes that are repeatedly and continuously committed by criminal organizations and generate large amounts of proceeds, and that legal person accounts controlled by criminal organizations are being misused as conduit accounts to conceal or transmit criminal proceeds.

In 2024, members of a criminal group were arrested for recruiting people to become representatives of shell company for rewards through social media, instructing them on how to set up legal persons and open legal person accounts, and laundering criminal proceeds using those accounts. It has become clear that this criminal group, claiming to operate as a receiving agent, managed approximately 500 shell companies and approximately 4,000 company accounts in an organized manner, and undertook ML of criminal proceeds from online and telephone fraud, social media-based investment fraud, online casinos, etc., committed by other criminal groups.

Table 44: Flow of Organized ML Involving Misuse of Legal Persons



(ii) Trends of STRs

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 substantially inactive company 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 identity 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 dormant*[1], a system intended to mitigate the risk of dormant companies that have been resold or whose registration has been illegally changed from being misused for crimes. ・Dissolution of dormant companies has been occurring every year since fiscal 2014, with approximately 30,000 cases in fiscal 2021, 29,000 cases in fiscal 2022, and 28,000 cases in fiscal 2023.

*[1] A stock company for which 12 years have elapsed since the day when activity regarding such stock company was last registered.

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, 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 the criminal proceeds, and there is a recognized risk that transactions with legal persons could be misused for ML/TF. In fact, in recent years, there have been cases of ML that appear to deliberately exploit the unique characteristics of legal persons, and it is considered that there is a high risk that transactions with legal persons similar to those mentioned in "(ii) Trends of STRs" above, could be misused for ML/TF.

In addition, looking at the characteristics of each type of legal person, existing stock companies are at risk of being misused due to their high credibility, but in recent years there have been cases of new stock companies being established and misused. As for membership companies, there is a risk that they will be misused by establishing new membership companies.

Furthermore, as the FATF points out, it is extremely difficult to trace funds attributed to legal persons, especially legal persons without transparency of beneficial owners, so transactions with legal persons without transparency of beneficial owners are recognized to be at high risk.

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. Major Products and Services in which Risk is Recognized*[1]

When assessing the risk, criminal environment described in "Section 2. Environment Surrounding Japan," major transactions misused for ML and 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. In addition, the assessment 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 regarding products and services.

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 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, including cross-border transactions
Convertibility	The convertibility of the source of funds by converting cash into other rights or goods, or by converting goods with high property value into cash
Complexity	Difficulty in tracing highly sophisticated and complex transaction types

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, funds transfer services, cryptoassets, and electronic payment instruments (expected to have a relatively higher risk)
Transactions considered to be of risk	Insurance, investment, trust, money lending, 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*[1]

(i) Factors that Increase Risks

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

Deposit-taking institutions such as banks must obtain licenses from the Prime Minister under the Banking Act, etc. As of the end of March 2024, 1,186 institutions have obtained the licenses, etc. They are mainly banks (134 banks, except branches of foreign banks) and cooperative financial institutions (254 Shinkin Banks, 143 Credit Cooperatives, 13 Labour Banks, 600 agricultural cooperatives and fishery cooperatives, and 42 credit federations of agricultural cooperatives and credit federations of fishery cooperatives). Among these institutions, banks held a total deposit balance*[2] of 1,180,232.2 billion yen for a total of 756.45 million accounts as of the end of March 2024.

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 expanding internationally. 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 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 recently

---

*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 which some cross-border crime organizations have transferred funds illegally obtained by fraud, etc., in foreign countries through Japan's financial institutions as part of their ML process.

Due to the characteristics mentioned above, the Financial Services Agency has assessed that the sector risk of deposit-taking institutions is "High," meaning that it is higher than that of other business types, in its financial sector analysis*[1]. Furthermore, among these, 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) Curren t situation of products/services provided by deposit-taking institutions and misusing cases

Looking at transactions misused for ML over the past three years, products and services provided by deposit-taking institutions are the most common.

(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. These days, it is possible 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, the convenience of savings deposit/savings accounts and the extensiveness of their use, based on their widespread popularity, 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 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 (Act No. 133 of 2007) 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

---

*[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.

The following cases are common examples of misusing deposit/savings accounts for ML:

- ○ Offenders used accounts belonging to other parties including foreign nationals 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.
- ○ 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 sale of fake brand goods.

Most of the modus operandi used for cleared cases of concealment of criminal proceeds involved deposits into accounts under the names of fictitious or other parties. There were more than a dozen accounts under the names of fictitious or other parties that had been misused in some past cases. Furthermore, hundreds of passbooks were seized from the crime base of a person arrested for soliciting the transfer of accounts. Accounts under the fictitious or other parties' names are the main criminal infrastructure of ML/TF, among others.

Most misused accounts are those under the names of individuals, such as accounts borrowed from a family member or friend, accounts purchased from a third party, and accounts opened under fictitious or other parties' names. There are also cases where deposit/savings accounts illicitly transferred from resident foreign nationals returning to their home countries are being misused for crimes. There are various modus operandi for illegally obtaining such accounts, and in recent years, criminal groups are soliciting account trafficking through social media. Certain characteristics can be identified, such as accounts under the names of debtors for a loan-shark being used for loan-shark crimes; Boryokudan members using accounts under the names of family members or friends for gambling crimes; and accounts under the names of fictitious or other parties being used for online and telephone fraud crimes.

There are also cases of accounts in corporate names being misused, including cases where accounts in corporate names are misused for crimes committed by organized crime groups that generate large amounts of proceeds, such as online and telephone fraud or cross-border ML offences.

Furthermore, the police actively cracks down on the following as contributors to the misuse of deposit/savings accounts (see Tables 45 and 46):

- ○ Violations of the Act on Prevention of Transfer of Criminal Proceeds related to the unauthorized transfer of deposit/savings accounts passbooks, cash cards, etc.
- ○ Fraudulent acquisition of savings account passbooks, etc., by deceiving deposit-taking institutions, such as by falsely stating the location of a postal receiving service provider's address as the residential address at the time of account opening (account fraud).
- ○ Receiving stolen property, knowing that it is a fraudulently obtained savings account passbook, etc.

When examining the violations of the Act on Prevention of Transfer of Criminal Proceeds in terms of the nationality, etc., of the suspects, Japan has the highest number of cases, followed by Vietnam

and China. However, compared to the number of foreign residents in Japan, the cleared cases of account transfer offences involving foreigners are conspicuous.

Given this situation and various case studies, it is apparent that the number of accounts being transferred significantly exceeds the number of cleared cases. It should be noted that ML/TF has been facilitated through the transfer of accounts.

Table 45: Number of Cleared Cases of Violating the Act on Prevention of Transfer of Criminal Proceeds

Category \ Year		2021	2022	2023
Transfer of deposit/savings passbook, etc.	(Number of cases)	2,446	2,951	3,230
Transfer of deposit/savings passbook, etc. (business)	(Number of cases)	27	18	43
Solicitation and inducement for transfer of deposit/savings passbooks, etc.	(Number of cases)	11	10	12
Transfer of exchange transaction cards, etc.	(Number of cases)	26	41	50
Transfer of information for cryptoassets exchange	(Number of cases)	23	46	89
Others	(Number of cases)	2	0	0
Total	(Number of cases)	2,535	3,066	3,424

Table 46: Number of Cleared Cases of Account Fraud etc.

Category \ Year		2021	2022	2023
Account fraud	(Number of cases)	710	733	726
Transfer of stolen goods	(Number of cases)	1	0	3
Total	(Number of cases)	711	733	729

Note: Based on reports on crimes that promote online and telephone fraud from prefectural police to the National Police Agency.

(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, characteristics of deposit/savings accounts, such as safe and reliable fund management, high convenience of deposit transactions, and the anonymity of transactions using cash withdrawn from deposit/savings accounts, are vulnerabilities for products and services and may allow persons who intend to commit ML/TF to do so through deposit transactions. 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 criminal proceeds that were 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 derived 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 caught for possessing the cash, and subsequently withdrew the money.
- An offender deposited some of the cash obtained through armed robbery into an account multiple times 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, 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 money, pretending that it was 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 which allow funds to be transferred easily, quickly, and over a wide area, is a vulnerability for products and services. In addition, 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 cases are common examples of misusing domestic exchange transactions 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 offender, through a business operator who did not know the situation.
- An offender logged into other persons' online brokerage accounts with illegally obtained account information and transferred the deposits in the accounts under the name of fictitious or other parties.
- 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 offender.
- 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 submitting a transfer request to a financial institution, and then had the funds further transferred from that acquaintance's account to the offender's account.
- In acquiring the proceeds from the sale of shares obtained by operating a Type I Financial Instruments Business without registration, an offender had the funds transferred to an account in the name of a general incorporated association under the offender's control, and then sent donation receipts to the customer, disguising the funds as a donation.
- 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 offender.

(d) Safe-Deposit Box

a. Current situation

A safe-deposit box is a lease of a depository. While anyone can operate safe-deposit box businesses, the service is generally known to be provided by deposit-taking institutions, such as banks, which lease out storage space in their branches for a profit.

Safe-deposit boxes of deposit-taking institutions are mainly used to store important documents, such as securities, bankbooks, bonds, deeds, or property, such as precious metals and stones. However, as deposit-taking institutions do not check the stored items, goods in safe deposit boxes offer a high degree of secrecy. As a result, there are cases where criminal proceeds derived from violating the Copyright Act and loan-shark crimes have been preserved in banks' safe-deposit boxes.

The characteristics of safe-deposit boxes, which allow safe storage of assets while maintaining confidentiality, are vulnerabilities for products and services. Therefore, safe-deposit box can be an effective means of physically concealing 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 make lease contracts for safe-deposit boxes with customers.

b. Typologies

Actual situations exist where persons attempting to commit ML/TF misuse safe deposit boxes as a physical way of storing criminal proceeds by leasing safe deposit boxes using fictitious or other parties' names.

The following cases are common examples 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 registered in the name of one of his family members.

(e) Bills and Checks

a. Current situation

Bills and checks are useful payment instruments that substitute for cash because they have high credibility with clearance systems or settlements by deposit-taking institutions. They are widely used in Japan's economy. Bills and checks are physically lighter than cash of equivalent value and are easy to transport. Also, it is easy to cash them through deposit-taking institutions. In addition, they are easy to transfer through endorsement and have high liquidity.

On the other hand, the characteristics of bills and checks, such as ease of transportation due to their lightweight shape, and the reliable convertibility into cash, are vulnerabilities for products and services. Therefore, bills and checks can be an effective means of receiving and concealing 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 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).

A checking account is necessary to draw bills or checks in general. The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct verifications at the time of transactions when opening accounts, and to prepare and preserve verification records and transaction records.

b. Typologies

Actual situations exist where persons attempting to commit ML/TF misuse bills and checks as a

way to transport the criminal proceeds easily or to disguise the proceeds as justifiable funds.

The following cases are common examples of misusing bills and checks for ML:

- ○ An illegal money-lending business operator made many borrowers draw and send checks, etc. by post for principal and interest payments. The checks were then collected by deposit-taking institutions and transferred to accounts opened in the name of fictitious or other party.
- ○ In accounting for promissory notes that were defrauded from business partners under the pretense of legitimate product sales, an offender forged delivery notes and invoices from fictitious suppliers, in order to make it appear that the proceeds were legitimate business earnings.

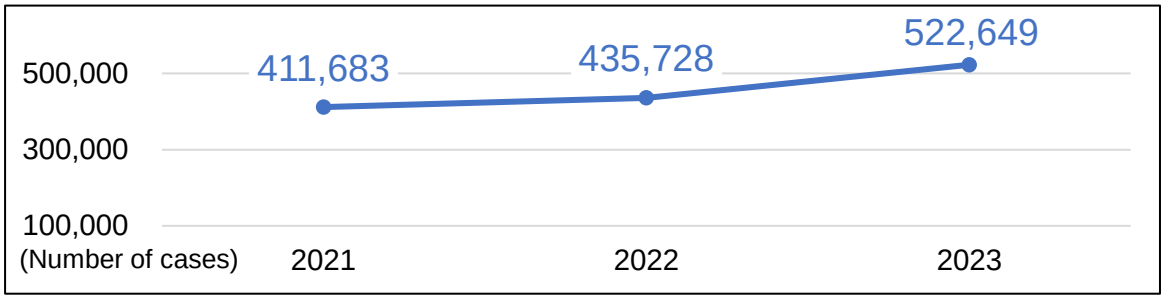
[Threats and Vulnerabilities Found by Competent Authorities in Recent Years]

- ・It was found in the receiving agent's scheme that there are business operators that obtain the 'rights to receive payments on behald 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"*[1]) to the said other business operators. There is a risk for banks, samely as for funds transfer service providers, that they cannot verify the identity of persons sending money to customers or persons who eventually receive funds.
- ・Cases of fraudulent transfers to financial institution accounts of cryptoassets exchange service providers have been confirmed. Although offenders and modus operandi have not been identified, there were cases where victims intentionally made funds transfers and cases where information of account created in the a cryptoassets exchange service provider was stolen from a victim and funds transfers were made against the victim's will.

(ii) Trends of STRs

Trends in the number of STRs submitted by deposit-taking institutions from 2021 to 2023 is as follows:

Table 47: Trends in the Number of STRs Submitted by Deposit-taking Institutions



The Financial Services Agency revised the "List of Reference Cases of Suspicious Transactions" for deposit-taking financial institutions by adding reference cases that focus on abnormal transactions specific to Internet-based transactions and financing of terrorism, and released it in March 2022.

*[1] So-called "bulk remittance" means a collective settlement payment that a business operator providing cross-border remittance services makes for several small remittance transactions between offices in Japan and abroad.

Among the guideline numbers and names in the Guidance for Submitting STRs*[1], the ones with the highest number of reports are as follows*[2]:

Table 48: Reporting Status of Major STRs by Deposit-taking Institutions

Reason for report	Number of reports	Percentage (%)
43. Customers with unusual behavior or movements	342,842	25.0
14. Frequent remittances from numerous individuals	134,386	9.8
42. Transactions related to Boryokudan gangsters or their related parties	132,243	9.7
16. Sudden large deposits, withdrawals and remittances	76,926	5.6
27. Large remittances from/to other countries for economically unreasonable purposes	76,339	5.6
1. Large cash transactions	62,955	4.6
11. Frequent large deposits, withdrawals and remittances	56,905	4.2
44. Unusual transactions based on the purpose, occupation or content of business	56,616	4.1
5. Transactions under fictitious or other party's name	42,887	3.1

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 service was being logged into from 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

In order to implement AML/CFT, each relevant law and regulation contains on measures to mitigate risks.

- ○ Act on Prevention of Transfer of Criminal Proceeds

  Stipulates that specified business operators are obligated to perform customer verification and other measures during 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

*1 "Guidance for Submitting STRs, 8th edition" by the National Police Agency (revised April 2024).

*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 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>

・Implemented lectures, training, and exchanges of opinions with other ministries and agencies, industry associations, and specified business operators to improve AML/CFT and enhance their systems.

<Ministry of Agriculture, Forestry and Fisheries>

・Issued orders for submission of reports on the development of systems including the facts about transactions and analysis of differences between the facts and the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in collaboration with the Financial Services Agency (about 670 cases) (March 2023).

・Revised the Comprehensive Guidelines for Supervision for Agricultural Cooperative Credit Business and the Comprehensive Guidelines for Supervision for Fishery Cooperative Credit Business in order to clarify the role of the central organization in AML/CFT measures for agricultural and fishery cooperative financial institutions (November 2023).

・Exchanged opinions on each service with persons in charge at all prefectural governments, regional agricultural administration offices, and industry associations, and once again promoted awareness of enhancing AML/CFT measures.

・Conducted inspections on subjects concerning compliance with the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism (including a risk-based approach) and system development.

<Ministry of Health, Labour, and Welfare>

・Collaborated with the Ministry of Finance and the Financial Services Agency to conduct targeted

ML inspections (3 Shinkin Banks) and supervision
- Notified again of the need to take action by the deadline for establishing internal control framework for AML/CFT measures.
- Collaborated with the Financial Services Agency to hold meetings to explain and exchange views on AML/CFT measures to Labour Banks' executive management (July and September 2023).

The Financial Services Agency has requested financial institutions, including those handling deposits, to complete the improvement of their management framework to enhance AML/CTF by March 2024, in accordance with the “Required actions for a financial institution” of “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism” published by the Financial Services Agency. The Financial Services Agency has received reports from most of the financial institutions that they have completed establishing internal control framework in accordance with the Guidelines, therefore, the Agency has evaluated that the intensive efforts under a deadline have had a certain effect. In addition, given that the deadline for establishing internal control framework has already passed, it is now necessary for financial institutions to advance their risk-based approaches and move on to a stage of enhancing the effectiveness of the frameworks. The Guidelines include provisions requiring financial institutions to verify the effectiveness of their frameworks for managing ML/TF risks. The Financial Services Agency plans to monitor the status of these verification efforts and to publish and share examples of frameworks and methods.

In addition, in August 2024, the Financial Services Agency and the National Police Agency jointly requested industry associations to take the following measures to prevent the illicit use of deposit/savings accounts, in order to combat against financial crimes committed through deposit/savings accounts:

(1) Strengthening fraud prevention and understanding of actual conditions at the time of account opening
(2) Multi-layered detection focusing on the validity of the user's access environment and the amount and frequency of transactions
(3) Enhancing and refining detection scenarios and thresholds focusing on the purpose of illegal use and the modus operandi
(4) Expediting detection and subsequent customer confirmation, as well as measures such as suspension of withdrawals, freezing, and contract termination
(5) Information sharing between financial institutions that contributes to the detection of signs of illicit use and the understanding of the actual situation.
(6) Strengthening information provision and collaboration with the police

(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.

[Examples of Initiatives Taken by Industry Associations and Specified Business Operators]* [1]

<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)
- A study session was held by the representative bank to introduce its initiatives (Regional Banks Association of Japan, Second Association of Regional Banks)
- Provided members with sample regulations related to risk management for ML/TF, and held an informational session (National Association of Shinkin Banks, National Central Society of Credit Cooperatives, National Association of Labour Banks)
- Summarized the progress of each Labour Bank toward the deadline for completing the establishment of internal control framework, and provided support to each Labour Bank as needed (National Association of Labour Banks)
- With the objective of standardizing AML/CFT measures within the agricultural and fishery cooperative system, provided a platform for transaction monitoring/filtering and basic customer information management, known as the systematic AML management system (Norinchukin Banks)

<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 financial 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.

---

* [1] 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. The same applies hereafter.

(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.

On the other hand, those 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 Attributes.*

- ○ Transactions under anonymous or fictitious, borrowed, and false 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 mitigating measures against these risks mentioned in the above (iii), in addition to statutory measures, and the outcomes of such measures can be seen from the effective efforts made by deposit-taking institutions.

---

*[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.

However, these efforts differ from one deposit-taking institution to another. Deposit-taking institutions that are 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). 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 are entities that, on behalf of banks etc., uses 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 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).

[Topic] Cooperation between Financial Institutions on Transaction Monitoring

In light of the digitization of finance and the sophistication of the modus operandi of ML/TF, the FATF requires each country to take measures at a higher level. It is an urgent matter for financial institutions to improve the effectiveness of AML/CFT.

It is pointed out that financial institutions that do not implement appropriate measures are generally at risk of ML and other offences.

Considering this situation, efforts are being made to enhance and streamline the core operations of AML/CFT in financial institutions, such as joint monitoring of transactions.

The Act to Partially Amend the Payment Services Act and Other Related Acts to Establish a Stable and Efficient Payment Services System, which was enacted on June 3, 2022, and promulgated on June 10, 2022 (effective June 1, 2023), established a system for "funds transfer transaction analysis service provider" that, upon request from multiple financial institutions, conduct the following tasks regarding exchange transactions:

- ○ Transaction filtering (to analyze whether customers are subject to sanction and notify the results of the analysis to financial institutions)
- ○ Transaction monitoring (to analyze whether transactions are suspicious and notify the results of the analysis to financial institutions)

Funds transfer transaction analysis business is a business that is contracted to conduct core operations of AML/CFT in financial institutions. Funds transfer transaction analysis service provider are expected to play a role in contributing to improving the effectiveness of AML/CFT in financial institutions, while ensuring a higher level of effectiveness of the transaction monitoring that they provide.

A licensing system has been introduced for funds transfer transaction analysis business, and as of the end of May 2024, 3 business operators have been licensed by the Commissioner of the Financial Services Agency under the Payment Services Act. Licensed operators are subject to inspection and supervision by the Financial Services Agency, etc., and the Financial Services Agency is supervising funds transfer transaction analysis service providers to ensure the quality of their operations, such as by publishing its guidelines.

> Comprehensive Guidelines for Supervision of Funds Transfer Transaction Analysis Providers
> https://www.fsa.go.jp/common/law/index.html (Financial Services Agency)

Financial institutions are required to take measures commensurate with their own risks, and the responsibility lies with the financial institutions themselves. Therefore, even when using a funds transfer transaction analysis service provider, financial institutions must not leave the work they have entrusted to them entirely to the provider, but must also check the quality of the services they receive and take additional measures as necessary.

(2) Insurance Dealt with by Insurance Companies, etc.[*1]

(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 damages caused by a certain incident. Payment is limited to cases where those conditions, which have uncertainty, are met. This characteristic significantly mitigates the risks insurance carries.

However, each insurance product varies in regard to its characteristics. Insurance companies 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 is particularly high if the premium allocation amount is refunded due to the cooling off.

This characteristic of the convertibility of the source funds into insurance products is a vulnerability for products and services and can be misused for ML/TF.

As of the end of March 2024, 97 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:

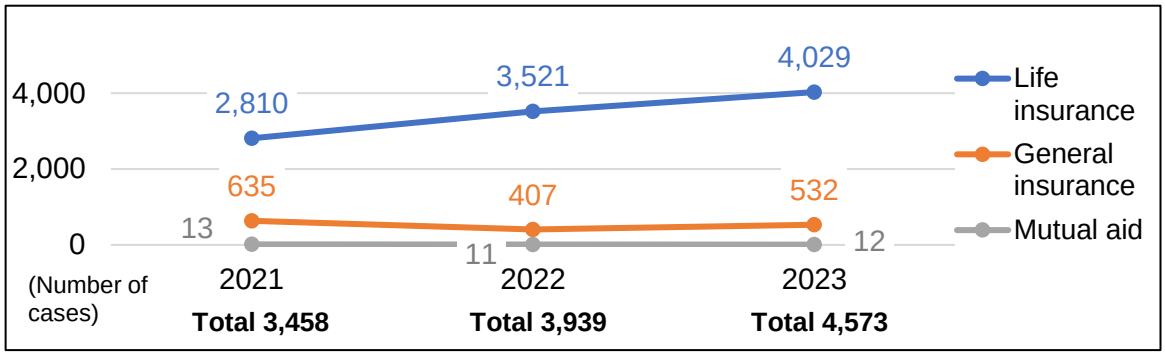
- An offender stole non-life insurance money for damages for missed work derived from fraud by making an insurance company transfer the money to an account in fictitious or other party's name.

(ii) Trends of STRs

Trends in the number of STRs submitted by insurance companies from 2021 to 2023 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 federation of fishery cooperatives) of the Act on Prevention of Transfer of Criminal Proceeds.

Table 49: Trends in the Number of STRs Submitted by Insurance Companies



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.

Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 50: 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	7,014	67.7
29. Customers with unusual behavior or movements	251	2.4

Table 51: 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	514	32.7
29. Customers with unusual behavior or movements	88	5.6
5. Transactions under fictitious or other party's name	58	3.7

(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, 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.

<Ministry of Agriculture, Forestry and Fisheries>
- Issued an order for submission of reports on the development of systems including the facts about transactions and analysis of differences between the facts and the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in collaboration with the Financial Services Agency (2 cases). (March 2023)
- Exchanged opinions on each service with persons in charge at all prefectural governments, regional agricultural administration offices, and competent associations engaging in mutual aid business, etc.
- Conducted inspections on subjects concerning compliance with the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism (including a risk-based approach) and system development.

(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 2023 projects, training and awareness-raising activities were conducted for agricultural cooperatives on measures, such as confirmation 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 high-savings schemes, new contract cancellations, and cooling-offs (transaction monitoring) to alert agricultural cooperatives about 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 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 2023 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 (Mutual Aid Federation of Fishery Industry Cooperative Associations).
- 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 (Mutual Aid Federation of Fishery Industry Cooperative Associations)
- Instructed Fishery Cooperatives to ensure that the prescribed identity verification 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 (Mutual Aid Federation of Fishery Industry Cooperative Associations).

(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 continuously 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, which may lead to sanctions in the event of violations, and establish a framework for accurately detecting high-risk customers.

(v) Assessment of Risks

Since insurance products with cash accumulation features enable criminal proceeds to be converted to immediate or 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 against these risks, in addition to statutory measures.

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*1

(i) Factors that Increase Risks

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

Besides deposits 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 in 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 2024, there were 5,691 financial instrument business operators registered by the Prime Minister or those notified to the Prime Minister based on the Financial Instruments and Exchange Act. The number of financial instruments 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) was 35.

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 2023 was about 944 trillion yen in the Prime Market, about 30 trillion yen in the Standard Market, and about 38 trillion yen in the Growth Market.

For commodity derivative transactions, the trading volumes amounted to approximately 2.75 million sheets*2 at the Tokyo Commodity Exchange and the Dojima Commodity Exchange in 2023.

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.

Meanwhile, 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.

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

---

*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.) and persons listed in item (xxxiii) of the same paragraph (commodity derivatives business operators).

*2 "Sheet" is the term for the minimum transaction unit showing transaction volume or delivery volume that constitutes the base for transactions in an exchange.

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.

In its financial sector analysis, the Financial Services Agency has assessed the sector risk of investment as "Low," which means relatively low.

(B) Typologies

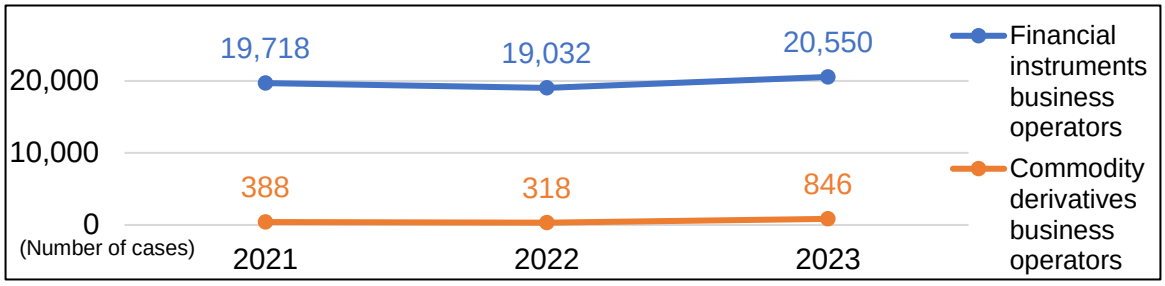
The following cases are common examples of products and services dealt with by financial instruments business operators and commodity derivatives business operators, as well as brokerage services for commissioned transactions on commodity markets that were misused for ML:

- 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 armed robbery into an account in his/her relative's name, deposited the criminal proceeds into an FX account opened in his/her relative's name as clearing margins.

(ii) Trends of STRs

Trends in the number of STRs submitted by financial instruments business operators, etc. and commodity derivatives business operators from 2021 to 2023 is as follows:

Table 52: Trends in the Number of STRs Submitted by Financial Instruments Business Operators, etc. and Commodity Derivatives Business Operators



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.

Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 53: Reporting Status of Major STRs by Financial Instruments Business Operators

Reason for report	Number of reports	Percentage (%)
4. Transactions under fictitious or other party's name	14,108	23.8
38. Customers with unusual behavior or movements	13,194	22.2
37. Transactions related to Boryokudan gangsters or their related parties	8,712	14.7

Table 54: 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	1,256	80.9

(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, and each relevant law and regulation contains provisions on measures to mitigate risks.

○ Financial Instruments and Exchange Act and Commodity 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/money.html (Ministry of Agriculture, Forestry and Fisheries) https://www.meti.go.jp/policy/commerce/z00/250701sakimono-shishin.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.
<Ministry of Agriculture, Forestry and Fisheries and Ministry of Economy, Trade and Industry>
・Conducted inspections on subjects concerning compliance with the Financial Services Agency's "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (including a risk-based approach) and system development.
<Ministry of Land, Infrastructure, Transport and Tourism>
・Issued orders for submission of reports on the development of systems, including the facts about transactions and analysis of differences between the facts and the guidelines in collaboration with the Financial Services Agency (82 cases). (March 2023)

(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]
・Conducted written surveys on the status of member companies' internal control framework and to collect 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).
・For the purpose of voluntary self-assessment by the members themselves, conducted follow-ups using the "Questionnaire on the Status of Compliance with Self-regulatory Rules," and shared the results to members to provide information and raise awareness. In the process, confirmed members' efforts of AML/CFT, including confirmation of their response to "Required actions for a financial institution" in the Financial Services Agency's "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (Japan Investment Advisers Association).
・Utilized online platforms to implement training for members (Japan Investment Advisers Association, Japan Securities Dealers Association, and Type II Financial Instruments Firms Association).
・Provided an overview of the Act on Prevention of Transfer of Criminal Proceeds and policies on verification of identity and other information during compliance training offered to members twice a year 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 foreign-national clients, implement appropriate measures, including verifying and retaining records of their residency status, 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 over-the-counter cash transactions, verify and document the reason for having to resort to such transactions 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 such split deposits or withdrawals. 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, and increase such obtained rights using 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].

In addition, 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, borrowed, or false 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 against these risks, in addition to statutory measures.

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. 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 307, and assets acquired using specified joint real estate venture schemes in fiscal year 2022 amounted to approximately 0.3 trillion yen, while assets transferred amounted to approximately 0.1 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 open accounts 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.*1

(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. 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 2024, 97 business operators were engaging in trust business with such a license and authorization.

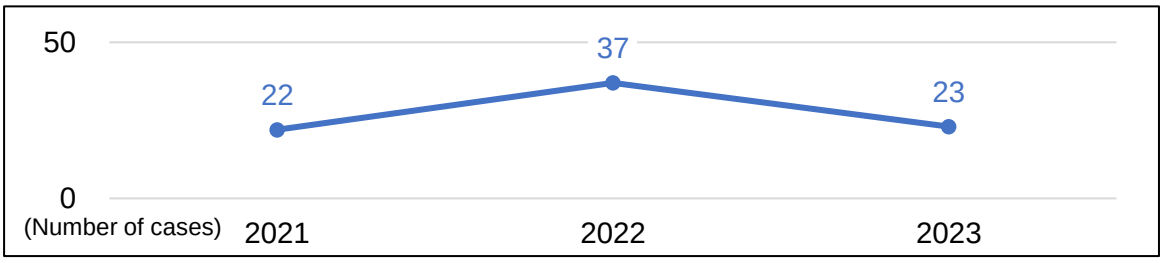
No cleared ML case involving the misuse of trusts has been reported in Japan in recent years. However, a trust have vulnerabilities for products and services, which are transferability in that a trust does not only mean leaving a property with a trustee but also changing the nominee of a property right 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

Trends in the number of STRs related to trust*2 between 2021 and 2023 is as follows:

Table 55: Trends in the Number of STRs Related to Trust



*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.

Among the types listed in *the List of Reference Cases of Suspicious Transactions*, the one with the highest number of reports are as follows:

○ Transactions that were conducted before the completion of CDD despite the customer being uncooperative, preventing the completion of CDD (28 cases, 34.1%).

○ Transactions related to Boryokudan gangsters or their related parties (15 reports, 18.3%).

(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, 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 CDD 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.

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 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 continuously 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 launching new trust products or services, take into account specific and individual risks for identifying and assessing the risks.
- ○ When analyzing the risks, conduct exhaustive and specific risk 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 altering 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 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 against these risks, in addition to statutory measures.

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.* [1]

(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, 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 2024, there were 1,515 registered business operators, while the outstanding balance of loans was 36.9641 trillion yen at the end of March 2023.

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

The following case is an example where criminal proceeds were transformed:

- Criminal proceeds from armed 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.

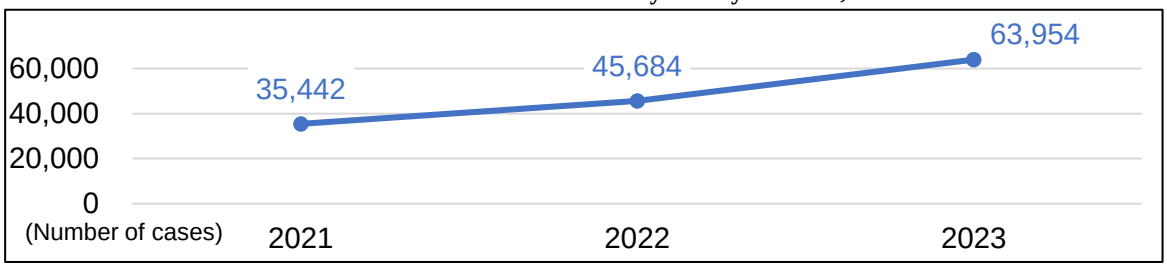
---

* [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

Trends in the number of STRs submitted by money lenders, etc., from 2021 to 2023 is as follows:

Table 56: Trends in the Number of STRs Submitted by Money Lenders, etc.



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.

Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 57: Reporting Status of Major STRs by Money Lenders

Reason for report	Number of reports	Percentage (%)
43. Customers with unusual behavior or movements	56,417	38.9
5. Transactions under fictitious or other party's name	48,863	33.7
42. Transactions related to Boryokudan gangsters or their related parties	10,538	7.3

(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, 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.

(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 when necessary, and prevent damage 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 continuously 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, borrowed, or false 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, in addition to statutory measures.

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) 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 means an exchange transaction service (registration of the appropriate remittance type that corresponds to the amount of each remittance required*[1]) provided 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 2024, there were 83 registered business operators. There were 2,341.29 million remittances totaling 7,575.6 billion yen in fiscal 2022. It is expected that the demand for and use of funds transfer services, which are used by foreigners in Japan who come from various countries as a less-expensive means of remittance than that offered by banks, is increasing as a new Internet-based payment method and will further increase in the future (see Table 58).

Table 58 Trends in Funds Transfer Service Business

Category \ Year		2020	2021	2022
Number of remittances per year		963,073,667	1,548,782,833	2,341,293,721
Breakdown	Domestic	892,640,092	1,473,790,829	2,263,357,787
	Cross-border	70,433,575	74,992,004	77,935,934
Transaction volume per year (million yen)		3,995,550	5,467,864	7,575,681
Breakdown	Domestic	2,595,589	3,989,725	5,902,381
	Cross-border	1,399,956	1,478,134	1,673,298
Number of registered funds transfer service providers		80	83	83

Note: Data from the Financial Services Agency

There are three main remittance 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 customers' accounts 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 the instrument.

Funds transfer services may involve a client giving face-to-face instructions to a funds transfer service provider to remit money, or also give non-face-to-face instructions to remit money by using mail, the Internet, etc. Recipients can receive payment, etc., in various ways, such as receiving cash or a money order

---

*[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.

and depositing it into a bank account. There is also a wide variety of remittance systems, and a variety of business models are being developed, including funds transfer service providers that have established systems for transferring funds internationally without using the remittance networks of deposit-taking institutions and provide services using their own unique methods of transferring funds. As a result, the nature of the risk differs for each funds transfer service provider, depending on the diverse services they offer, such as the transparency of cross-border remittances. Specifically, there is a decline in transparency regarding cross-border remittances when appropriate AML/CFT measures commensurate with the business model are not in place. Starting from April 2023, it has become possible for funds transfer service providers to submit applications for designation to the Minister of Health, Labour, and Welfare, enabling wage payments into accounts at funds transfer service providers, thus expanding the range of services that funds transfer service providers can offer.

Funds transfer services have characteristics, including transferability, which allows funds to be moved quickly and reliably on a global scale at low fees; extensiveness, which allows funds to be transferred to foreign countries with different legal systems and transaction systems; and anonymity through non-face-to-face transactions. These characteristics reduce traceability. By misusing such vulnerabilities of products and services, funds transfer services can be an effective means of ML/TF.

In its financial sector analysis, the Financial Services Agency 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 for all global operations and did not establish appropriate regulations or procedures to verify identity and other information, 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

With the introduction of funds transfer services, it became easier to remit money overseas with reasonable fees. Some people came to misuse the services to commit ML/TF by disguising their remittances as lawful ones. The following cases are common examples of misusing funds transfer services for ML:

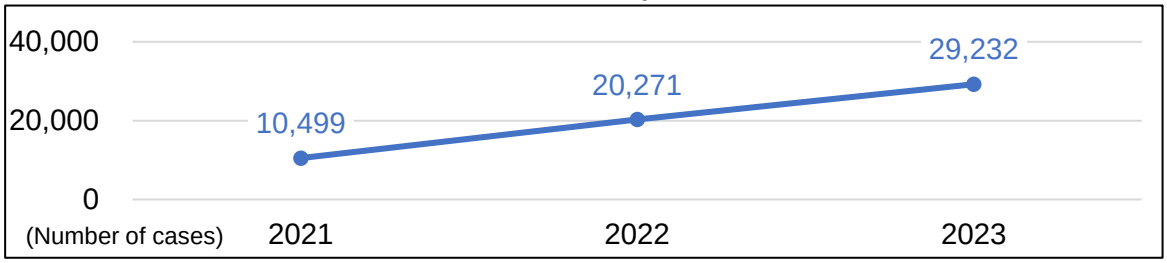
- ○ A dangerous drugs trafficker concealed his proceeds in an account opened in fictitious or other party's name, and then paid for the procurement of materials to produce drugs from overseas using funds transfer services.
- ○ A foreigner illegally staying in Japan after the expiration of his authorized 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.
- ○ An offender made their victim remit criminal proceeds from fraud carried out by a foreign crime organization to a bank account in Japan and then made the victim transfer the proceeds 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, 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

Trends in the number of STRs submitted by funds transfer service providers from 2021 to 2023 is as follows:

Table 59: Trends in the Number of STRs Submitted by Funds Transfer Service Providers



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.

Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 60: 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	15,778	26.3
15. Sudden large deposits, withdrawals and remittances	6,506	10.8
4. Transactions under fictitious or other party's name	3,662	6.1
16. Economically unreasonable transactions	3,613	6.0
42. Transactions related to Boryokudan gangsters or their related parties	2,647	4.4

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

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, 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>
Held multiple study sessions through the Japan Payment Service Association, 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" (from January 2023 to March 2024).

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 finds transfer service providers are found to be lagging behind in their efforts, 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 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.

(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 damages, 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 damage where malicious third parties open accounts with funds transfer service providers using illegally obtained depositor information in the depositors' names, link these accounts with bank accounts, deposit funds from the bank accounts to the funds transfer service provider's accounts, and make unauthorized withdrawals (fraudulent use involving bank account impersonation). Also, incidents where third parties, having obtained the information of funds transfer service IDs and passwords illicitly, use funds transfer services against the users' will without authorization (fraudulent use involving payment account hijacking) were disclosed (Japan Payment Service Association, August 2023 and March 2024).
- Created materials summarizing the content of the lectures and training sessions held eight times over the course in fiscal 2023 to enhance AML/CFT measures and released them to members (Japan Payment Service 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 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 continuously 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 withdrew money by depositing 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), the use of 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.

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, borrowed, and false 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

Against such a risk background, the competent authorities and funds transfer service providers are taking statutory measures, as a matter of course, and 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.

(7) Electronic Payment Instruments Dealt with by Electronic Payment Instruments Service Providers*[1]

(i) Factors that Increase Risks

In recent years, amidst the digitalization of finance, transactions using so-called stablecoins*[2], 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 March 2022, amendments to the Payment Services Act and other laws were submitted to the 208th session of the National Diet. These amendments introduce business regulation, such as a registration system for electronic payment instruments service providers, and include electronic payment instruments service providers as specified business operators under the Act on Prevention of Transfer of Criminal Proceeds. The bill was enacted on June 3 of the same year, published on June 10, and came into effect on June 1, 2023, following the establishment and amendment of subordinate laws and regulations.

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, among other necessary regulations, to ensure appropriate user protection and ML/TF measures while 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.
- ○ These 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.
- ○ 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

---

*1 Entities listed in Article 2, paragraph (2), items (xxxi-xxxii) of the Act on Prevention of Transfer of Criminal Proceeds (electronic payment instruments service providers).

*2 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).

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 issuance of electronic payment instruments has not been confirmed in Japan as of the end of September 2024, 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.

(ii) Measures to Mitigate Risks

(A) Statutory measures

In order to implement 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.

- Financial Instruments and Exchange Act and Payment Services Act

  Excludes certain trust benefits corresponding to electronic payment instruments from the application of the Financial Instruments and Exchange Act and applies the regulations of the Payment Services Act and others to issuers such as trust companies.

- 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 (effective April 1, 2024).

(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) 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 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 is 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, borrowed names, or false 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 implement statutory measures but also advance the establishment of ML/TF countermeasure systems equivalent to those of cryptoassets exchange service providers, which includes 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 new entrants that have not implemented appropriate ML/TF countermeasures, indicating the need for continuous measures to reduce risks.

(8) 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 2024, there are 29 registered business operators.

The transaction amounts in cryptoassets are increasing globally, including in Japan, leading to the occurrence of cases related to cryptoassets. July 2019 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 in recent years in terms of the threats surrounding cyberspace. For example, the number of cleared cases of cybercrimes in 2023 was a record high of 12,479 cases, damage 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.

Meanwhile, in Japan, measures are being taken to enhance the environment against cyber attacks against cryptoassets exchange service providers, including the amendment of the Payment Services Act in May 2019, which mandated the segregation of customer assets (management in cold wallets not connected to the network).

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 moving cryptoassets from the blockchain it is recorded on to another blockchain.

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 identity verification measures are not mandatory, 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 bitcoins via cryptoassets ATMs using forged identification documents, it is necessary to see how such ATMs are actually being used.

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

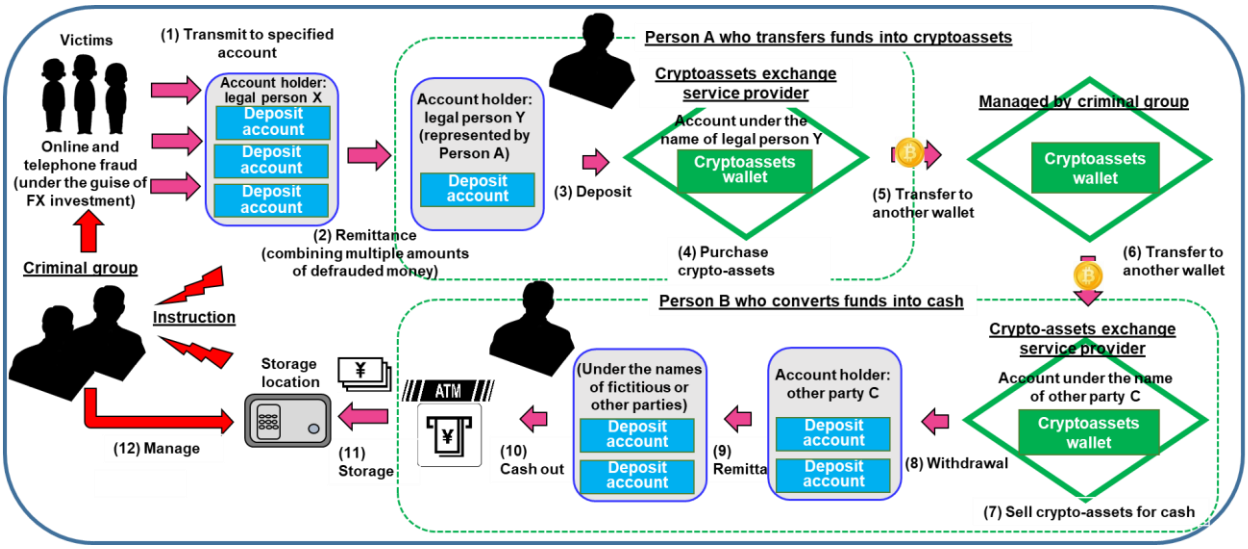
The following cases are common examples of misusing cryptoassets for ML:

- 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 offender so they could be withdrawn in cash.
- An offender transferred cryptoassets obtained through computer fraud to a cryptoassets wallet at a foreign cryptoassets exchange 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 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 an unknown person.

Table 61: Flow of Money Laundering Involving Abuse of Cryptoassets



The following cases are common examples of the rising violations of the Act on Prevention of Transfer of Criminal Proceeds, 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:

- A case where an offender provided IDs and passwords for cryptoassets accounts opened by foreign students and workers, etc., who were allowed to stay in Japan only during their authorized period of stay, to a third party with charge.
- A case where an offender opened accounts with cryptoassets exchange service providers using the principal identification documents of a fictitious or other party.

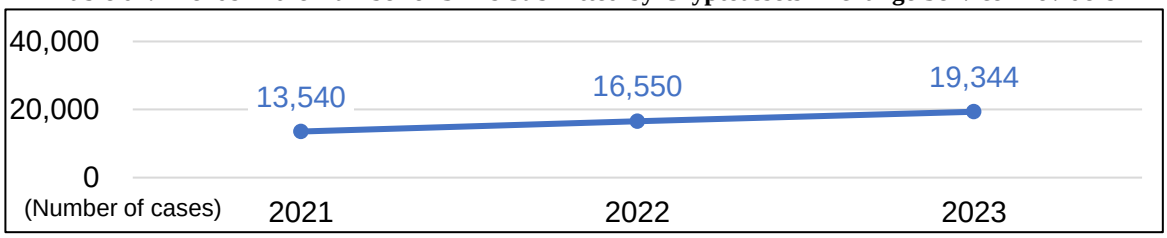
Furthermore, the following cases are common examples of using cryptoassets as payment in criminal cases:

- 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.

(ii) Trends of STRs

Trends in the number of STRs submitted by cryptoassets exchange service providers from 2021 to 2023 is as follows:

Table 62: Trends in the Number of STRs Submitted by Cryptoassets Exchange Service Providers



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.

Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 63: Reporting Status of Major STRs by Cryptoassets Exchange Service Providers

Reason for report	Number of reports	Percentage (%)
41. Customers with unusual behavior or movements	6,569	13.3
34. Refusal to provide true beneficiary explanations and materials	5,221	10.6
2. Frequent in a short-term, with large total amount of cash	4,175	8.4
4. Transactions under fictitious or other party's name	3,644	7.4
35. Transactions in which the true beneficiary is suspicious	1,673	3.4

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 service was being logged into from outside 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

In order to implement 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 checks to be conducted 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 compliance standards for foreign exchange transactions service providers and stipulated the obligation to establish internal control framework of asset freezing measures (effective April 1, 2024).

(B) Measures by competent authorities

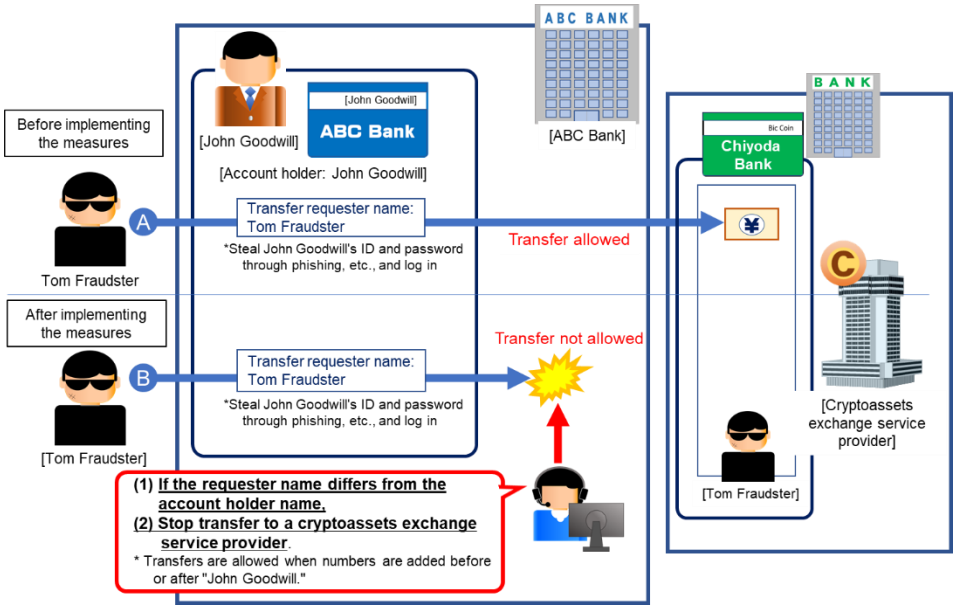
To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training for industry associations and specified business operators.

In addition, since February 2023, there have been a large number of cases involving fraudulent online banking transfers believed to be the result of phishing, in which funds are transferred to the financial institution accounts of cryptoassets exchange service providers, as well as cases of online and telephone fraud in which funds are made to be transferred to the financial institution accounts of cryptoassets exchange service providers. In light of this, the National Police Agency and the Financial Services Agency have requested industry associations for deposit-taking institutions to further strengthen their measures against fraudulent transfers to cryptoassets accounts, referring to the following examples.

○ Suspension of transfers to cryptoassets exchange service providers due to name changes

○ Strengthening monitoring of fraudulent transfers to cryptoassets exchange service providers

Table 64: 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>

- Held multiple study sessions through the Japan Virtual and Cryptoassets Exchange Association, 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"
- Conducted outreach to industry associations and business operators, in response to the enforcement of the cryptoassets transaction notification obligation (so-called travel rule) under the Act on Prevention of Transfer of Criminal Proceeds and the publication of the FATF report*[1] on the cryptoassets sector.
- 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.

(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.

*[1] The contents of the report are described in "Section 5 1. (8) [Topic] International Trends Surrounding Cryptoassets" in this NRA-FUR.

[Examples of Initiatives Taken by Industry Associations and Specified Business Operators]
<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 continue to 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 legal requirements such as verification at the time of transaction, and beyond quoting the contents of 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 high-risk 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 based on the identification and assessment of risks conducted internally, including management of the period of stay of foreign nationals.

(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 transferring 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, borrowed, or false 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 the development of a system that includes measures to mitigate the degree of risks mentioned above, in addition to taking statutory measures. 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. The competent authorities and industry associations continue to give guidance for maintaining the standards and continue to take measures to mitigate risks. For example, they urge new business operators who have not taken appropriate AML/CFT 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 timely and appropriately due 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.

[Topic] International Trends in Cryptoassets

Since the FATF Recommendation for cryptoassets and cryptoassets exchange service providers (Recommendation 15) was finalized in June 2019, the FATF has been monitoring compliance with the FATF standards by the public and private sectors and consulting with industry associations to publish information on the progress, facts, and issues every year. The FATF adopted a roadmap in February 2023 and, as part of that, published "Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity*1" in March 2024, which includes a table listing the implementation status of Recommendation 15 in FATF member jurisdictions and jurisdictions with important virtual asset service provider (VASP)*2 activity. The FATF and the VACG (Virtual Asset Contact Group) will continue to provide outreach and assistance to support global compliance with Recommendation 15 and plan to update the table in 2025.

The report "Virtual Assets: Targeted Update on Implementation of the FATF Standards*3" published in July 2024 points out the following issues regarding cryptoassets:

- ○ Comparing the results of the 2023 survey on the implementation status of FATF Recommendation 15 on cryptoassets in each country, global implementation remains relatively insufficient, although progress has been made or is being made in introducing regulations related to MF/TF, including in some jurisdictions with important VASP activity.
- ○ Regarding the travel rule, more than half of the jurisdictions that responded to the survey have taken measures toward implementation, but there has still been insufficient progress.

The report also points out that cryptoassets are not only being used to support the proliferation of weapons of mass destruction, but are also continuing to be used by fraudsters, terrorist groups, and other illicit actors. For example, North Korea continues to steal or extort cryptoassets from consumer and citizen victims and is increasingly using sophisticated methods to launder these illicit proceeds. Cryptoassets are also increasingly being used by terrorist groups, particularly ISIL in Asia and groups in Syria, who are known to often seek to use stablecoins or conceal their assets in cryptocurrencies to enhance anonymity.

Furthermore, there have been cases of increased fraudulent use of stablecoins for ML/TF purposes and continued hacking of decentralized finance (DeFi*4) arrangements. On the other hand, certain progress was reported regarding the use of smart contracts as a risk mitigation measure. In addition, progress in regulation, supervision and enforcement was also reported in some jurisdictions, such as the introduction of regulations regarding ML/TF and proliferation financing, including travel rule requirements for stablecoin service providers, taking regulatory and enforcement action against DeFi arrangements, and conducting risk assessments of unhosted wallets, including DeFi and peer-to-peer transactions.

The FATF and VACG has set up secretariats for FATF-style regional bodies (FSRBs), as well as global standards, and by working with the relevant international organizations that provide support and training, continue to undertake outreach and assistance to encourage compliance with Recommendation 15, particularly in jurisdictions with low capacity and important VASP activity. In addition, they will continue to share knowledge, experiences and challenges regarding the implementation of Recommendation 15, such as those related to unhosted wallets, including DeFi and peer-to-peer transactions, and will monitor market developments in this area to identify any developments that may require further FATF efforts.

---

*1 "Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity" (March 2024)

*2 In "Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity" and "Virtual Assets: Targeted Update on Implementation of the FATF Standards," cryptoassets are referred to as Virtual Assets (VA) and cryptoassets exchange service providers are referred to as Virtual Asset Service Providers (VASP).

*3 "Virtual Assets: Targeted Update on Implementation of the FATF Standards" (July 2024)

*4 Decentralized Finance. While there is no clear definition for what is commonly referred to as “DeFi,” the Financial Stability Board (FSB)’s report from February 2022 describes it as “financial services and products intended to operate without intermediaries, based on distributed ledger technology.”

As described above, it is necessary to continuously pay attention to the risks of ML/TF in cryptoassets transactions in light of the difference in efforts made by countries toward regulation of cryptoassets, changes in the markets that occur as a result of introduction of new technologies, and other issues.

(9) 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 65).

Table 65: Transactions by Foreign Currency Exchange Operators

Reporter \ Year		2021				2022				2023			
		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	Megabank (Note 2)	4	12,062	6,738	559	4	43,663	15,781	361	4	102,487	24,639	240
	Regional Bank	72	12,560	3,036	242	63	31,131	5,377	173	49	55,296	5,695	103
	Shinkin Bank	70	534	65	121	53	1,489	168	113	38	951	109	114
	Foreign Bank	19	232	97	418	20	252	369	1,465	20	254	974	3,832
	Other (Note 3)	6	7,465	726	97	6	4,294	662	154	6	13,005	1,063	82
Businesses Other Than Deposit-taking Institutions	Funds Transfer Business/ Credit Card Business	11	19,420	5,096	262	9	74,288	17,432	235	9	160,582	22,219	138
	Hotel Business	19	65	17	261	18	847	147	173	20	6,580	1,352	205
	Travel Business	10	149	64	429	12	431	96	223	13	2,438	186	76
	Secondhand Articles Dealer Business	36	10,225	1,965	192	42	23,296	3,416	147	58	40,404	4,664	115
	Airport-related Business	3	6,339	432	68	3	26,610	1,540	58	4	74,027	3,972	54
	Passenger Ship-related Business	-	-	-	-	-	-	-	-	1	239	2	1
	Large-scale Retail Business	1	13	0.3	25	1	37	1	36	2	175	6	34
	Other	41	27,500	9,742	352	42	54,966	8,158	148	50	138,501	11,893	86
Total		292	96,564	27,978	290	273	261,304	53,147	203	273	594,937	76,773	129

Note 1: 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.
2: Megabank in this table are Mizuho Bank, Sumitomo Mitsui Banking Corporation, MUFG Bank, and Resona Bank.
3: Shinkin Central Bank, credit associations, Japan Post Bank and other banks.

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 for 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 do it. 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)

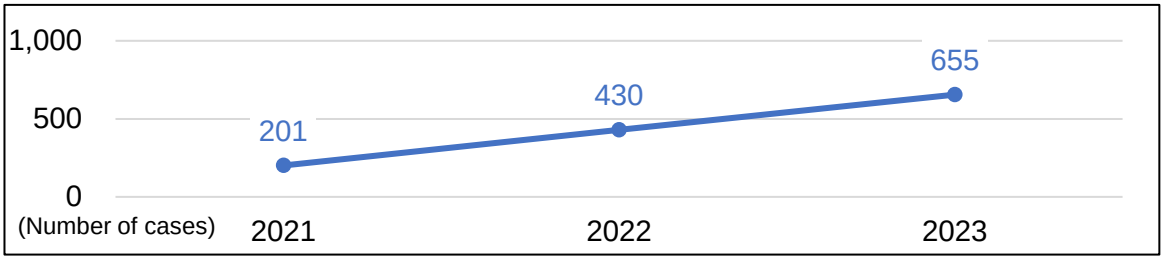
In addition, although not handled by currency exchange operators, there was the following case where foreign currency exchanges between individuals have been misused for ML:

- 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

Trends in the number of STRs submitted by foreign currency exchange operators from 2021 to 2023 is as follows:

Table 66: Trends in the Number of STRs Submitted by Foreign Currency Exchange Operators



The Ministry of Finance revised *the List of Reference Cases of Suspicious Transactions* for foreign 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.

Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 67: Reporting Status of Major STRs by Foreign Currency Exchange Operators

Reason for report	Number of reports	Percentage (%)
3. Frequent transactions in a short term	380	29.5
1. Large cash transactions	252	19.6

(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, 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>

・Pursuant to the amendment of the FEFTA, the "Compliance Standards for Foreign Exchange Transactions Service Providers" was established, mandating foreign exchange transactions service providers to take risk-based measures for dealing with economic sanctions and to establish internal control framework. In response to this, the Ministry of Finance promulgated the "Ministerial Ordinance Establishing Compliance Standards for Foreign Exchange Transactions Service Providers," which stipulates specific compliance matters related to the compliance standards. (Promulgated on May 26, 2023, and effective on April 1, 2024)

・Following the establishment of the above compliance standards, formulated and published the " Guidelines for Foreign Exchange Transactions Service Providers on Compliance with the Foreign Exchange Act and Its Regulations, etc." and Q&A, which summarize the actions required of foreign exchange transaction service providers to comply with the FEFTA and related regulations.

(Published on November 24, 2023)
・Held multiple explanatory sessions for industry associations, currency exchange operators, regarding the measures required under the revised FEFTA and the above guidelines.

(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 should be carried out at the time of transaction.
- ○ 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 information 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, which is highly liquid 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, borrowed, and false 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, statutory measures as a matter of course, the above-mentioned risk-mitigating measures against 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.

(10) 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.

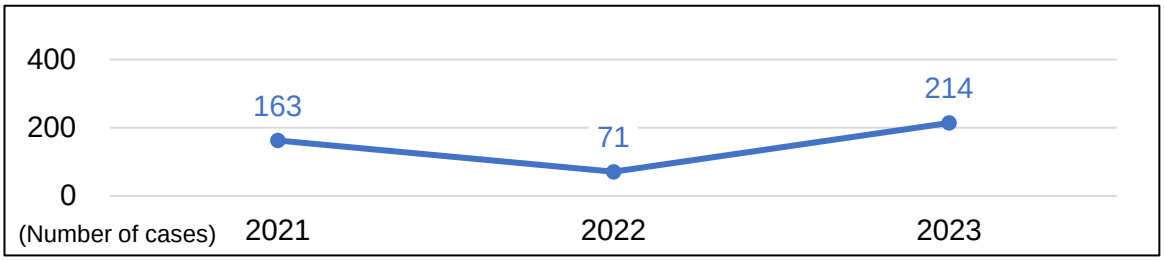
(B) Typologies

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

Trends in the number of STRs submitted by financial leasing operators from 2021 to 2023 is as follows:

Table 68: Trends in the Number of STRs Submitted by Financial Leasing Operators



Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 69: 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	272	60.7
8. Empty lease	51	11.4

(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.

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 the Japan Leasing Association to thoroughly inform member companies of "Notification of transactions suspected to be related to Taliban affiliates," and the association informed member companies accordingly.
- Conducted outreach to 4 financial leasing operators to confirm the current status of AML/CFT measures in financial leasing operators.
- Conducted risk assessments of financial leasing operators against ML/TF, and considered formulating guidelines for financial leasing operators by the Ministry of Economy, Trade and Industry.

(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 information to be verified at the time of transactions, etc. and providing training.

Respective financial leasing operators also take measures to prevent risks from transactions that carry a high risk of 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, 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.leasing.or.jp/guideline.html (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 continue to consider for AML/CFT measures are as follows:

- 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, borrowed, and false names (including suspected ones)
- Transactions related to financial leasing in which it is suspected of defrauding a financial leasing operator out of money under multiple financial leasing contracts
- Transactions related to financial leasing in which it is suspected that a lessee, etc., intends to defraud a financial leasing operator out of money by concluding several leasing contracts based on the same facilities

Competent authorities and financial leasing operators are taking, statutory measures as a matter of course, the above-mentioned risk-mitigating measures against 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.

(11) 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 2024, 246 operators were registered.

In recent years, with the spread of e-commerce and cashless payments, the credit card payment market has been continuously expanding. On the other hand, with the increase in cyber crimes as a background, the damage from fraudulent use of credit cards is expanding, reaching a record high of 54.09 billion yen in 2023.

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 providing a 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*[2].

(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 use the funds 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.

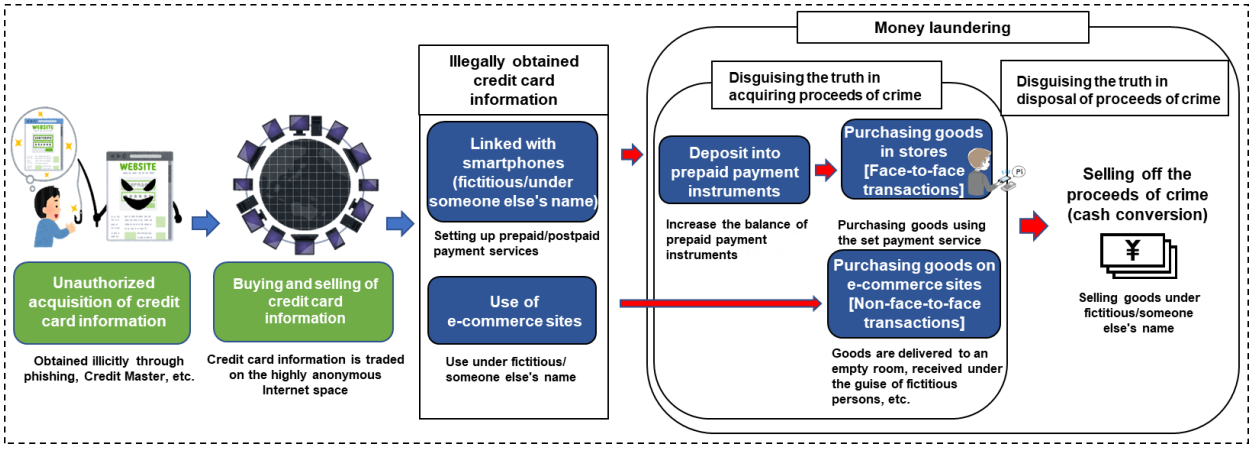
---

*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).

*2 "Report of the Study Group on Ensuring Safety and Security in a Cashless Society," by the Cyber Affairs Bureau of the National Police Agency(March 2024)

- 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 e-money usage rights (prepaid payment instruments) 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 fraudulent use of the payment service to acquire 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.

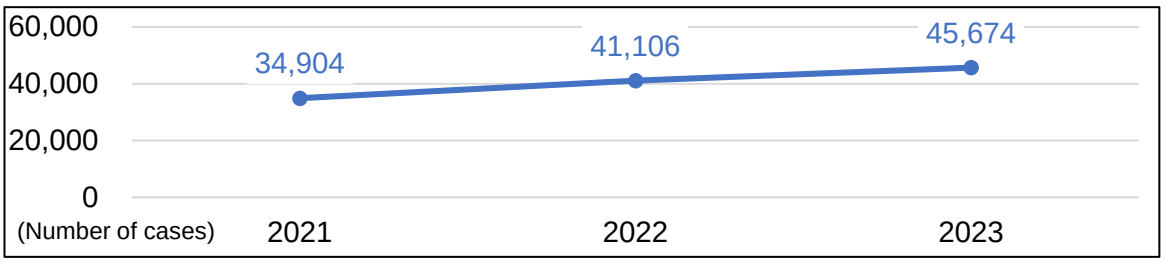
Table 70: Image of ML Misused by Credit Cards



(ii) Trends of STRs

Trends in the number of STRs submitted by credit card operators from 2021 to 2023 is as follows:

Table 71: Trends in the Number of STRs Submitted by Credit Card Operators



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.

Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 72: Reporting Status of Major STRs by Credit Card Operators

Reason for report	Number of reports	Percentage (%)
9. Use of cards by those different from the nominees	34,589	28.4
3. Transactions under fictitious or other party's name	27,623	22.7
13. Customers with unusual behavior or movements	17,735	14.6
12. Transactions related to Boryokudan gangsters or their related parties	14,147	11.6

(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, 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 of identity and other information 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 continue to 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 obtained in cash 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, borrowed, and false 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 statutory measures as a matter of course, the above-mentioned risk-mitigating measures against 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.

(12) 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 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 in cash transactions 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 the Building Lots and Real Estate Brokerage Act (Act no. 176 of 1952). There were approximately 130,583 brokers as of the end of March 2024. In 2022, the annual amount of sales was about 46 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 2023, was about 180,000. 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

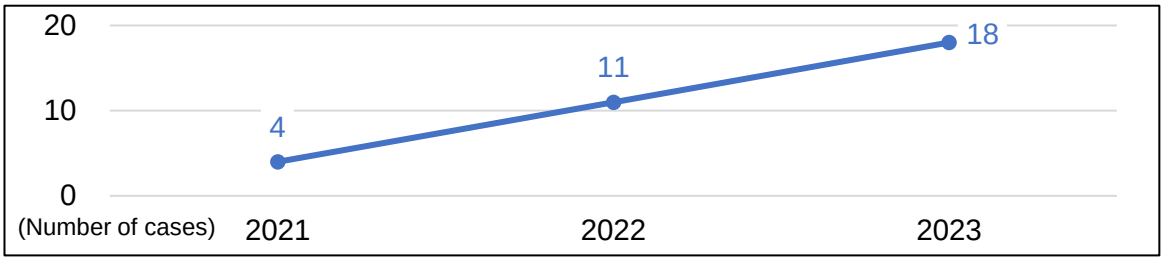
The following cases are common examples of misusing real estate for ML:

- 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 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)

(ii) Trends of STRs

Trends in the number of STRs submitted by real estate brokers from 2021 to 2023 is as follows:

Table 73: Trends in the Number of STRs Submitted by Real Estate Brokers



Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 74: Reporting Status of Major STRs by Real Estate Brokers

Reason for report	Number of reports	Percentage (%)
1. Large cash transactions	16	48.5
20. Customers with unusual behavior or movements	3	9.1

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

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, 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 check 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 2023 was 1,225).

(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 review of 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]
- Revised the "Handbook for preventing transfer of criminal proceeds in the real estate business" and disseminated it to member companies (Liaison Council for Preventing Transfer of Criminal Proceeds and Damage Caused by Anti-social Forces in Real Estate Business)
- Concluded an agreement with the Kanagawa Prefectural Police on measures to prevent the transfer of criminal proceeds and conducted training to deepen mutual understanding (Kanagawa Prefectural Headquarters of the All Japan Real Estate Association, Kanagawa Prefectural Real Estate Transaction 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 real estate brokers should continue to consider for AML/CFT measures are as follows:

- When conducting verification at the time of transaction, confirm identification data 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).

(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, borrowed, or false 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, statutory measures as a matter of course, the above-mentioned risk-mitigating measures against 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.

(13) 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

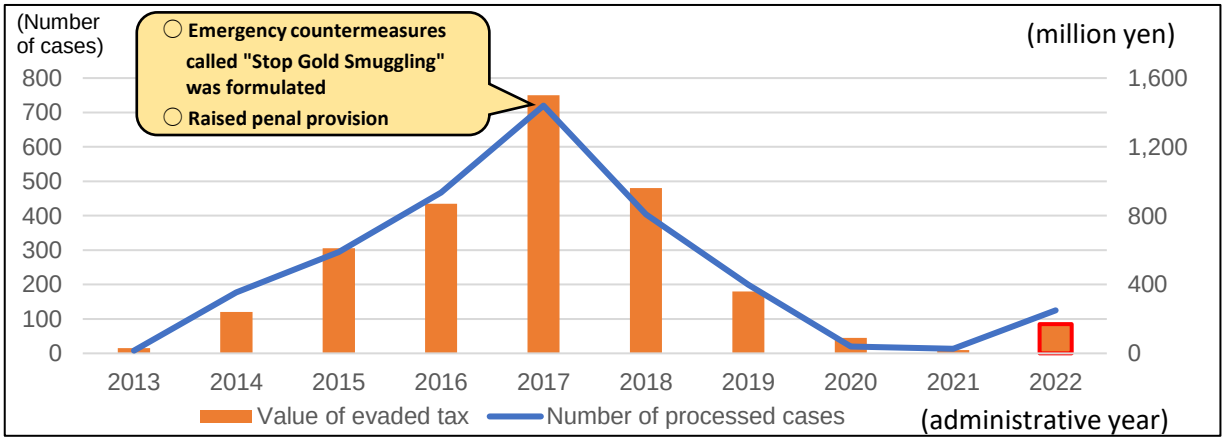
Precious metals and stones have high financial value and are easy to carry because of their small size. They can be easily exchanged with a large amount of cash in any region in the world. In addition, the distribution channel or location of the sold and purchased jewelries and precious metals hard to trace, so they are highly anonymous. As such, the characteristics such as anonymity of the source funds in cash transactions, high financial value, global marketability, 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 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 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 2022 administrative year*[2], the number of processed cases (notifications and indictments) of gold smuggling was 125 (approximately 9.6 times compared to the previous administrative year), and the value of evaded taxes was about 170 million yen (approximately 8.2 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 had been decreasing. However, gold smuggling is on the rise again due to factors such as the rising price of gold and the recovery of inbound tourism after the end of border measures to prevent the spread of COVID-19, so future trends should be closely monitored.

Table 75: Number of Processed Cases of Gold Smuggling and the Value of Evaded Tax



*[1] Means precious metals set forth in Article 6, paragraph (1), item (x) of the FEFTA.
*[2] The period from July 2022 to June 2023.

The modus operandi of smuggling has been sophisticated, 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, clothes, etc. Meanwhile, smuggling routes have diversified, including the use of airline passengers, air freight, and international mail. When looking in terms of the source of smuggling, Hong Kong, Korea, Vietnam, and Taiwan 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 trafficking 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 one of the reasons why 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 changed to only accepting 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 other person.

These transactions were conducted with an increased level of anonymity, by impersonating to other person or falsifying identification data, etc.,through the presentation of forged IDs at the time of the conclusion of contracts on purchase. Besides abroad, there was

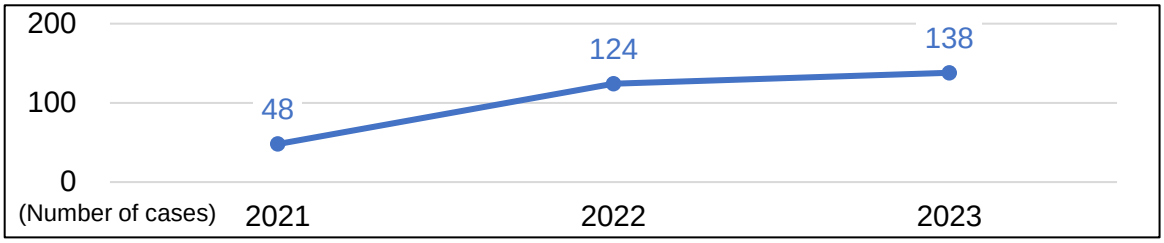
- A case where an offender purchased gold bullion using criminal proceeds derived from drug crimes and smuggled them to foreign countries

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

Trends in the number of STRs submitted by dealers in precious metals and stones from 2021 to 2023 is as follows:

Table 76: Trends in the Number of STRs Submitted by Dealers in Precious Metals and Stones



Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 77: Reporting Status of Major STRs by Dealers in Precious Metals and Stones

Reason for report	Number of reports	Percentage (%)
1. Large cash transactions	77	24.8
2. Frequent in a short-term, with large total amount of cash	31	10.0
17. Frequent in a short-term, multiple transactions	30	9.7

(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, 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. 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, etc. 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>
- Requested industry associations to thoroughly inform member companies of "Notification of transactions suspected to be related to Taliban affiliates," and industry associations informed member companies accordingly.
- 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. (November 2023)

(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 Jewelry Association makes efforts to ensure that member companies understand AML/CFT measures by preparing and distributing leaflets and guidebooks 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, 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.

Dealers in precious metals and stones are making efforts to establish and strengthen their internal control systems to prevent money laundering by regularly getting external audits to acquire international industry certifications, maintaining regulations and manuals, and conducting regular training.

(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 continue to 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, borrowed, and false 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.

Against such risks, competent authorities and dealers in precious metals and stones are executing statutory measures as a matter of course, 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.

(14) 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 4 reports in accordance with the Act on Prevention of Transfer of Criminal Proceeds from postal receiving service providers between 2021 and 2023. 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, occupations of customers, etc.
- 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 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

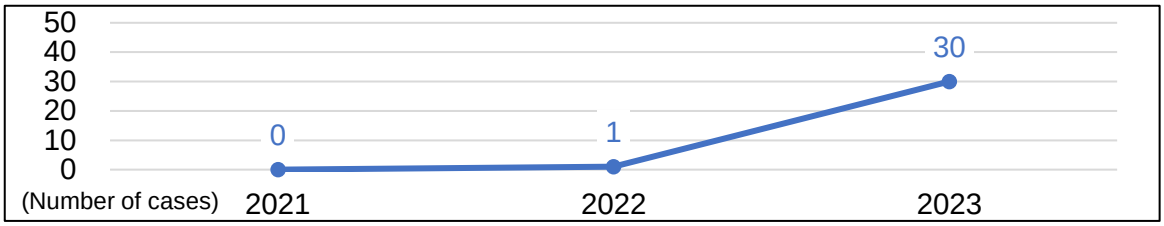
The following cases are common examples of misusing postal receiving services for ML:

- 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

Trends in the number of STRs submitted by postal receiving service providers from 2021 to 2023 is as follows:

Table 78: Trends in the Number of STRs Submitted by Postal Receiving Service Providers



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.

Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 79: 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	8	25.8
9. Customers with unusual behavior or movements	1	3.2

(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 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 check 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, and 2 cases of guidance for postal receiving service providers.

Following the receipt of reports and statements based on the results gathered by the National Public Safety Commission, the Ministry of Economy, Trade and Industry has been collecting reports and providing specific guidance based on the Act on Prevention of Transfer of Criminal Proceeds to the concerned businesses. In 2023, no corrective orders were issued to postal receiving service providers.

(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 continue to 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 data is 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, borrowed, and false 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 who often receive large amounts of cash

Against such risks, competent authorities and postal receiving service providers need to take, statutory measures as a matter of course, 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.

(15) 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.

The Ministry of Internal Affairs and Communications assesses that telephone receiving service providers that conduct non-face-to-face verification at the time of transactions, and other telephone receiving service providers with few workers that have not established a management system, in particular, are high risk of being misused for ML/TF.

(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 2021 and 2023 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 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 check 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>

- Conducted 1 case of reporting collection and 2 cases of guidance for telephone receiving service providers (2023)
- 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. (January 2024)
- 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)

(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 receiving service providers should continue to 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.

(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 statutory measures, as a matter of course, the abovementioned mitigating measures against 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.

(16) 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 2024, 978 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, 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 17 reports from telephone forwarding service providers in accordance with the Act on Prevention of Transfer of Criminal Proceeds during the period from 2021 to 2023. The details of major violations of obligations discovered as a result of collecting the reports in 2023 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.

The Ministry of Internal Affairs and Communications evaluates that, in particular, telephone forwarding

---

*[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.

service providers that conduct non-face-to-face verifications at the time of transactions, those with few employees that do not have appropriate systems, and those that purchase telephone lines from other companies are at a high risk of misuse for ML/TF.

(B) Typologies

The following case is an example of misusing a telephone forwarding service for ML:

- In 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.

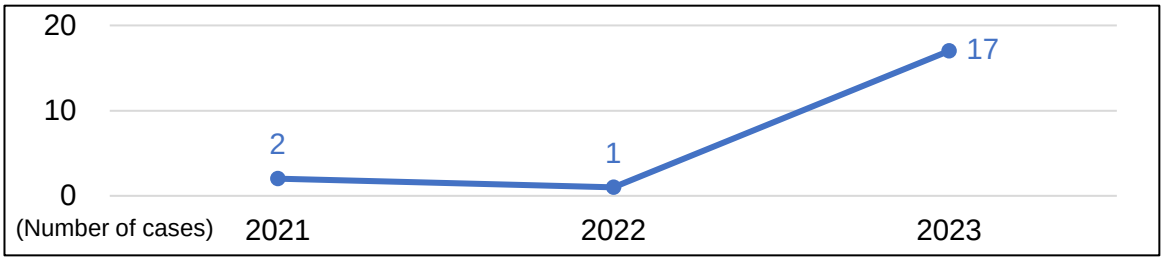
As the above case shows, telephone forwarding services are misused as a means to conceal the owner of the criminal proceeds.

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 a online and telephone fraud.

(ii) Trends of STRs

Trends in the number of STRs submitted by telephone forwarding service providers from 2021 to 2023 is as follows:

Table 80: Trends in the Number of STRs Submitted by Telephone Forwarding Service Providers



Among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 81: Reporting Status of Major STRs by Telephone Forwarding Service Providers

Reason for report	Number of reports	Percentage (%)
1. Intent to masquerade as the actual status of the company, etc.	1	5.0
5. Transactions under fictitious or other party's name	1	5.0

In addition, 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, 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 check 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 implementing 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 identified through the above scheme, implemented the measure to suspend inventory numbers in bulk for 3,270 numbers from 4 providers in 2023.
- Conducted 2 cases of reporting collection and 1 case of guidance in accordance with the Act on Prevention of Transfer of Criminal Proceeds (2023).
- 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. (January 2024)
- 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 (November 2023).

Following the receipt of reports and statements based on the results gathered by the National Public Safety 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 2023, no corrective orders were issued to telephone forwarding service providers.

In light of the actual situation identified by the competent authorities, the key points to which telephone forwarding service providers should pay attention are as follows:

- ○ Checking the purpose of transactions and occupations of customers
- ○ Checking corporate customers for beneficial owners
- ○ Creating and saving verification records
- ○ Sending transaction-related documents by registered mail that must not be forwarded or the like in non-face-to-face transactions
- ○ Referring to *the List of Reference Cases of Suspicious Transactions* and considering the necessity for submitting STRs regarding transactions conducted by the company

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.

Offenders 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 began implementing 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 used for fraud, in addition to landline numbers, subject to

measures such as 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 government agencies, providing members with the latest information, and issuing warnings (Japan Unified Communications Service Provider 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 telephone forwarding service providers should continue to consider for AML/CFT measures are as follows:

- 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, borrowed, or false names (including those suspected to be such names) are at a higher risk.

Competent authorities are taking measures against such risks 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.

(17) Legal/Accounting Services Dealt with by Legal/Accounting Professionals[*1]

(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, etc., provide legal services at the request of a client or other person concerned. Lawyers, etc., 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 2024, 45,808 lawyers, 3 Okinawa special members, 493 foreign lawyers, 1,691 legal profession corporations, and 9 foreign legal profession corporations are registered in Japan.

Judicial scriveners, etc., 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, etc., 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 2024, 23,156 judicial scriveners, etc., and 1,194 judicial scrivener corporations are registered.

Certified administrative procedures legal specialists, etc., 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, etc., 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 2024, 51,619 certified administrative procedures legal specialists and 1,356 certified administrative procedures legal specialist corporations are registered.

Certified public accountants, etc., 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, etc., 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 2024, 35,558 certified public accountants, 2 foreign certified public accountants, and 287 audit firms are registered.

Certified public tax accountants, etc., 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, etc., 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

---

[*1] Legal/accounting professionals mean lawyers, etc., judicial scriveners, etc., certified administrative procedures legal specialists, etc., certified public accountants, etc., and certified public tax accountants, etc.

the end of March 2024, there were 81,280 certified public tax accountants and 5,002 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, they can use their high social credibility to lend the appearance of legitimacy to dubious transactions and asset management 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 getting legal or accounting professionals who have social credibility involved 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 legal person, 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.

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 Identity, etc. with regard to certain transactions, the retention of 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 Identity, etc. and retention of records and other matters.

Table 82: 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 data</th><th>Confirmation of transaction purposes</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 is 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 among legal and accounting professionals.

(a) Japan Federation of Bar Associations (JFBA) and Regional Bar Associations

The JFBA implemented amendments to its rules, including the addition of verification items beyond the identification of clients (such as the purpose of the request, occupation/business content, ultimate beneficial owners, and asset and income status in the case of high-risk transactions) and the explicit consideration of the Risk Assessment for Money Laundering in Legal Practice (hereinafter referred to as “Legal Practice Risk Assessment for ML”) in March 2023, and notified its members of the revision in preparation for the enforcement in April 2024. Furthermore, in order to encourage lawyers, etc., to understand the 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, 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 JFBA's 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 amendment of the Act on Prevention of Transfer of Criminal Proceeds in December 2022, 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 also created and distributed a "Guideline for the Risk-Based Approach (Concepts)" and a leaflet to inform clients of the amendments of the Act on Prevention of Transfer of Criminal Proceeds.

In light of the actual situation identified by the competent authorities, judicial scriveners, etc., should pay attention to the following matters for AML/CFT measures:

- Appropriately verify clients' identities 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

JFCAPLSA has posted a training program titled “Identity Verification under the Act on Prevention of Transfer of Criminal Proceeds” on the VOD training website for member administrative scriveners, etc., since January 2018 to ensure that all members properly conduct identity verifications and prepare transaction records to prevent the transfer of criminal proceeds.

Furthermore, since March 2019, JFCAPLSA has announced their obligations, such as the obligation to verify the identity 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 amendment of the Act on Prevention of Transfer of Criminal Proceeds in December 2022, 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 is considering revising the "Act on Prevention of Transfer of Criminal Proceeds - Identity Verification Handbook" published for certified administrative procedures legal specialists, etc.

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.
- Appropriately create and save confirmation records.

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 formulated and published 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 publication 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 JICPA annually conducts a survey of certified public accountants, etc., on their compliance with the Act on Prevention of Transfer of Criminal Proceeds, and also provides e-learning courses and introduces publications on ML/TF issued by the FATF on its member website. In addition, the JICPA held training sessions for its members, inviting external experts, to give an overview of the Act on Prevention of Transfer of Criminal Proceeds and the need for AML/CFT measures. Furthermore, following the enforcement of the amended Act on Prevention of Transfer of Criminal Proceeds on April 1, 2024, JICPA published a new research report with the aim of supporting its members in smoothly fulfilling the various obligations stipulated in the Act on Prevention of Transfer of Criminal Proceeds. It also released a video commentary for members on AML/CFT measures required of certified public accountants, etc., based on details of the amendment. Additionally, the JICPA disseminates information on AML/CTF to its members via email.

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 the transaction and create and save confirmation records and transaction records.
- 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 amendment of the Act on Prevention of Transfer of Criminal Proceeds in December 2022, 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 distributing leaflets on AML/CFT Measures for Certified Public Tax Accountants to all their member certified public tax accountants, etc., and by revising the guidelines on the internal control systems for certified tax accountant offices.

In light of the actual situation identified by the competent authorities, certified public tax accountants, etc., should pay attention to the following matters for AML/CFT measures:

- Conduct verification at the time of transaction and appropriately create and save 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, borrowed, or false 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 mitigating measures against these risks, in addition to statutory 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 Using New Technologies That Should Be Monitored Closely

(1) High-Value Electronically Transferable Prepaid Payment Instruments Dealt with by Issuers

(i) Factors that Increase Risks

(A) Characteristics

Prepaid payment instruments refer to vouchers, numbers, symbols, or other codes (including those whose value is recorded on computers or servers) issued in advance in exchange for payment. They can be used for purchasing goods, borrowing, or paying for services from issuers or affiliated stores. Primarily used as a means of micropayment at specific services or affiliated stores, the total issuance amount of prepaid payment instruments in 2022 reached 29.4665 trillion yen*[1].

There are two types of prepaid payment instruments: “prepaid payment instruments for their own business,” which can only be used for payments to the issuer, and “prepaid payment instruments for third-party business,” which can also be used for payments at affiliated stores. The Payment Services Act mandates that issuers of prepaid payment instruments for their own business with unused balances exceeding a certain amount must notify the Prime Minister, and issuers of prepaid payment instruments for third-party business must register with the Prime Minister.

Furthermore, among prepaid payment instruments for third party business, those capable of electronic value transfer and allowing high-value deposits and transfers are now regulated as “high-value electronically transferable prepaid payment instruments” by the Act to Partially Amend the Payment Services Act and Other Related Acts to Establish a Stable and Efficient Payment Services System, enacted in June 2022. Specifically, issuers of high-value electronically transferable prepaid payment instruments must submit a business implementation plan to the regulatory authority in advance as mandated by the Payment Services Act, and those who have submitted such notification are to be added as specified business operators under the Act on Prevention of Transfer of Criminal Proceeds, and are subject to obligations such as verification at the time of transaction.

Generally, under the Payment Services Act, refunds of unused balances purchased are prohibited, except in cases of the issuer's closure, preventing users from freely withdrawing cash equivalent to the deposited amount*[2]. However, with the utilization of online platforms and international credit card payment infrastructures, prepaid payment instruments that can be used for a wide range of goods and services at various stores have emerged, making their functions closely resemble cash despite the restriction against redemption claims against issuers.

---

*1 See the Japan Payment Service Association website for “Trends in Issuance Amounts of Prepaid Payment Instruments.”

*2 Even if they function as prepaid payment instruments, 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 transaction verification.

(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 a virtual prepaid card (prepaid payment instruments) created online under a fictitious name or the name of other party, which was then used for payment of living expenses, and also was transmitted to a newly created virtual prepaid card 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 (prepaid payment instruments) registered under a fictitious identity was increased.
- Products were purchased in stores using electronically obtained electronic money rights (prepaid payment instruments) of other party, impersonating the holder.
- Using a cash card obtained illegally, an offender operated an ATM to withdraw cash, then used the cash to purchase electronic money rights (prepaid payment instruments), and transferred the electronic money rights by sending the code number of the electronic money rights to another person via social media.
- A business operator that purchases electronic money rights (prepaid payment instruments) pretended to be a legitimate business when purchasing electronic money rights that had been stolen in online and telephone fraud, and then sold the electronic money rights via an online intermediary.
- An offender purchased electronic money rights (prepaid payment instruments) that had been stolen in online and telephone fraud from another offender who ran an electronic money trading business, and then sold the electronic money rights to an electronic money buying business, owned by the offender, pretending to be someone else.

(ii) 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, 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 for ensuring AML/CFT, 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 crime victimization 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.

[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) 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. Currently, many issuers set a maximum deposit limit and restrict the use of deposited amounts to specific affiliated stores. However, with the advancement of cashless payments, the availability of prepaid payment instruments, including online stores, has expanded, and their forms and methods of use are diverse. Furthermore, because identity verification is not required for use, they can be considered to have a high degree of anonymity.

In fact, there have been cases where prepaid payment instruments were misused in the ML process, with an increasing trend in such incidents. Particularly in cases of online and telephone fraud, criminals deceive victims into giving away their electronic money rights (prepaid payment instruments) and then conceal the criminal proceeds by selling the stolen electronic money rights (prepaid payment instruments) through websites that mediate the sale and purchase of electronic money.

Regarding high-value electronically transferable prepaid payment instruments, 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 prepaid payment instruments. These international brand prepaid payment instruments, 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, which suggests that they could be considered to have at least the same risk level from an ML/TF perspective.

(2) 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 pointed out the ML methods and techniques in casinos as follows:

- Purchasing chips with criminal proceeds and cashing them out without playing.
- 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

---

*[1] Vulnerabilities of Casinos and Gaming Sector (March 2009)

- ○ Provision of premiums related to casino gaming (so-called “complimentary”) in which the value of the premiums 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.

[Topic] Report on ML and International Organized Crime Related to Online Casinos

There are countries/regions where online casinos are legally operated. However, even if they are legal in the country/region where they are operated, it is a crime to connect to them and gamble from within Japan. In recent years, it has been pointed out that the number of accesses to foreign online casino websites has increased, and there have been cases where gamblers and business operators claiming to be payment agents located in Japan have been arrested.

In a report published in January 2024*[1], the United Nations Office on Drugs and Crime (UNODC) Regional Office for Southeast Asia and the Pacific warned that international organized crime in Southeast Asia has been rapidly developing and expanding in recent years by incorporating the latest information technology. Among other things, the report pointed out the following matters regarding ML by criminal organizations through the misuse of online casinos.

1. Recent situations regarding casino-related ML in Southeast Asia and surrounding regions
   - ○ Casinos and junkets*[2] have for years served as vehicles for regional underground banking and ML.
   - ○ In recent years, the use of online payment technology and blockchain technology has led to a rapid increase in sophisticated online gambling platforms, including online casinos, allowing for faster anonymized movement of funds by organized crime groups.
   - ○ Organized crime groups use advanced information technologies such as data mining and artificial intelligence to commit cyber-related crimes, making their crimes more sophisticated and international. Online casinos are supporting these crimes.
   - ○ According to latest available segment forecasts, online gambling market is projected to grow further between 2022 and 2026, with the Asia Pacific region representing the largest share of market growth.
   - ○ These new systems have helped expand the booming illicit economy, in turn attracting new networks, innovators, and service providers, therefore it will be important to pay close attention to future developments.
2. Characteristics and modus operandi of ML using online casinos

Online casinos have the characteristics that it is easy to set up with limited technical expertise and overhead capital, irrespective of gambling laws within a given jurisdiction. The online gambling sector is also characterized by a non-face-to-face element, minimal, if any, compliance staff, and huge and complex volumes of transactions and financial flows, which are often international in nature.

Modus operandi of ML misusing online casinos include the following:

Modus operandi	Details
Cash-in cash-out	A criminal exchanges their money for playing chips and then converts them back into cash. This is the simplest, most typical method of laundering money at a casino.
Collusion between players	Proceeds of crime are deliberately lost in a game, in a way that benefits an accomplice who acts as another player in the same game.
Junket financing (mirror transactions)	A criminal use junkets in one country/region as a gambler/client, to deposit criminal proceeds into the junket account as funds for playing. Then the criminal play at a casino through the same junket in another country/region, effectively transferring funds. Junkets may also provide a high interest rate to individuals willing to store their money with the junket, providing so-called "safekeeping" transactions.
Misuse of gambling accounts	Gambling accounts provided by casinos are used like traditional bank accounts to make and receive payments.

*[1] Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat

*[2] A junket is an agent that invites players to casinos, and is an important factor in increasing sales and profits for casino business operators. (Materials from the 7th meeting for promotion of development of specified integrated resort districts)

Section 6. Low-risk Transactions

This section describes transactions with low risk.

According to 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.

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

*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.

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, paragraph (1), item (vi), (b) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	(i), (iii), (iv), (vi)
		Individual Credit*4, 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)

*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.

*4 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.

		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 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	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*1	(iii), (viii)
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.*2)	(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)	(i), (iii), (iv), (viii)

*1 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).

*2 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.

		(b) of the Ordinance of the Act on Prevention of Transfer of Criminal Proceeds	
		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.*1	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 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.