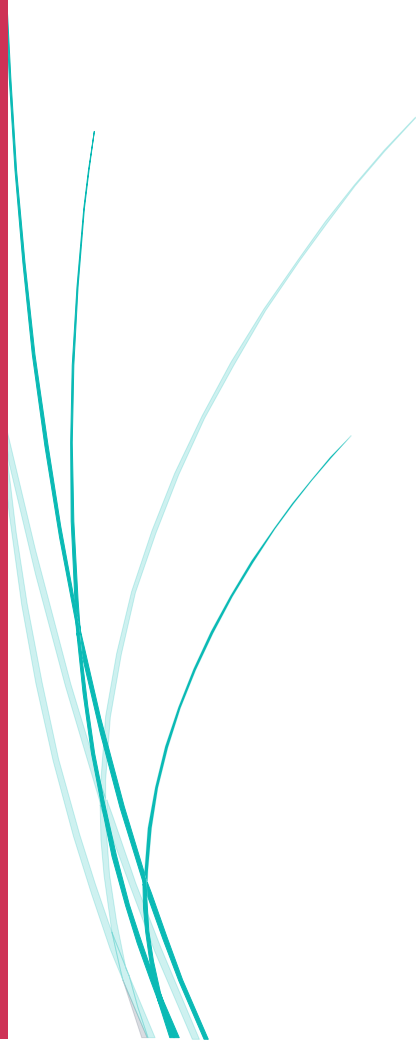
December 2023

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 Offenses 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 on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007)
Enforcement Order	Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds (Cabinet Order No. 20 of 2008)
(the) Ordinance	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)

Introduction

1. History

In modern society, where information technology and globalization of economic/financial services are advancing, the state of money laundering*[1] and terrorist financing (hereinafter referred to as "ML/TF") are constantly changing. In order to strongly cope with the problem, global countermeasures are required through the cooperation of countries.

In the 40 Recommendations revised in February 2012 (hereinafter referred to as the "FATF Recommendations"), the Financial Action Task Force (FATF) made a series of requests to countries, including a request to identify and assess ML/TF risks within their borders.

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.

Since then, pursuant to the provisions of Article 3, paragraph 3 of the Act on Prevention of Transfer of Criminal Proceeds*[2] which were newly established when the act was revised in 2014, the National Public Safety Commission has prepared and published National Risk Assessment-Follow-up Report (hereinafter referred to as a "NRA-FUR"), that describes risks, etc. in each category of the transactions carried out by specified business operators*[3], etc. in keeping with the contents of the NRA-Baseline Analysis*[4].

2. Purpose

The FATF Recommendations (Recommendation 1) 1 calls on each country to identify and assess their own ML/TF risks, and the Interpretive Notes to the FATF Recommendation request business operators to take appropriate steps to identify and assess ML/TF risks with respect to their products and services to implement appropriate Anti-Money Laundering and Countering the Financing of Terrorism (hereinafter referred to as "AML/CFT") measures with a risk-based approach.

In order for specified business operators in Japan to accurately determine whether the transactions or customers are subject to suspicious transactions of ML/TF in the huge number of transactions, it is effective to apply a risk-based

---

*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 Law.

*2 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.

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

*4 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. This 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 of this NRA-FUR include terrorist financing risks.

approach (e.g., applying enhanced customer due diligence (CDD) to higher risk transactions, applying simplified CDD to lower risk transactions). As a prerequisite for the risk-based approach, specified business operators need to accurately understand the risks in the transactions they carry out. Accordingly, the National Public Safety Commission, which is in a position to gather, arrange, and analyze information relating to the transfer of criminal proceeds (hereinafter referred to as "criminal proceeds") or concerning suspicious transactions, has prepared and published an NRA-FUR describing the risks for each category of transaction carried out by specified business operators. Expert knowledge and information have been obtained from administrative authorities supervising specified business operators (hereinafter referred to as "competent authorities") concerning the characteristics of their products/services or the status of their AML/CFT systems or controls, etc.[*1]

In order to carry out verification at the time of transactions, etc. accurately, the Act on Prevention of Transfer of Criminal Proceeds and its related Ordinance[*2] require specified business operators to take measures to keep up-to-date information for which verification at the time of transactions was conducted, and make effort to prepare the document prepared by specified business operators, etc. by considering the details of the NRA-FUR. Specified business operators are required to implement appropriate AML/CFT measures through a risk-based approach. Specifically, specified business operators are required to understand and take into account the reasons why the transactions handled by them, which are described in the NRA-FUR, are considered as posing a risk or high risk when they perform their own risk assessment commensurate with their own business categories, scales, etc. In addition, it is necessary to take into account not only the NRA-FUR but also the contents of guidelines established by the competent authorities. When a transaction is conducted with a specified business operator, it is also useful to look into factors affecting the degree of risk and the status of the AML/CFT systems, relating to the products and services handled by the transaction counterpart as described in the NRA-FUR.

3. Overview of NRA-FUR

In Section 2 of this NRA-FUR, a broad range of risks surrounding Japan is outlined from the perspectives of geographical, social, and economic environments and criminal circumstances. Section 3 analyzes the offenders of ML/TF, such as Boryokudan(Japanese organized crime groups), Online and telephone fraud groups, and Crime groups of foreigners in Japan. It also examines major predicate offences, including theft, frauds, drug-related crimes, and transactions that are misused for ML/TF.

In Section 4 of the NRA-FUR, transactions with a high level of risk are evaluated based on transaction type, countries/regions, and customer attributes. Section 5 assesses products and services that are relatively higher risk.

---

*1 Article 3, Paragraph 4 of the Act on Prevention of Transfer of Criminal Proceeds stipulates that when deemed necessary for the aggregation, organization, and analysis of information as per the provisions of Paragraph 2, and for the investigation and analysis as per the provisions of the preceding paragraph, the National Public Safety Commission may request relevant administrative agencies, specific business operators, and other related parties to provide documents, express opinions, give explanations, or any other necessary cooperation.

*2 Article 11 of the Act on Prevention of Transfer of Criminal Proceeds and Article 32 of the Ordinance.

[Overview of NRA-FUR]

○ **General Risk Assessment**

Environment Surrounding Japan
1. Geographic environment 2. Social environment 3. Economic environment 4. Criminal circumstances, etc.

○ **Individual Risk Assessment**

Analysis of Money Laundering Cases, etc.		
Offenders	**Modus Operandi**	**Suspicious Transaction Report**
1. Boryokudan 2. Online and telephone fraud groups 3. Crime groups of foreigners in Japan	1. Predicate offences (thefts, frauds, etc.) 2. Major transactions misused for money laundering, etc.	1. Number of notifications by business type

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

Transaction Types	**Countries/Regions**	**Customer Attributes**
1. Non-face-to-face transactions 2. Cash transactions 3. Cross-border Transactions	1. Countries/regions against which the implementation of countermeasures are requested by the FATF Recommendations (particularly high-risk) Iran and North Korea 2. Countries/regions subject to applying enhanced due diligence measures proportionate to the risks arising from the jurisdiction (high-risk) Myanmar, (Result of the June 2023 FATF Plenary)	1. Boryokudan, etc. 2. International terrorists (Islamic extremists, etc.) 3. Non-residents customers 4. Foreign politically exposed persons 5. Legal Persons (legal persons without transparency of beneficial owners, etc.)

○ **Risk Assessment (ii): Products and services**

Products and services			
Transactions of relatively higher risk than other business forms	● Products and services dealt with by deposit-taking financial institutions ● Funds transfer services ● Crypto assets	**Transactions that are expected to have a relatively higher risk compared to other business forms**	● Electronic payment instruments
Transactions considered to be of risk	● Insurance ● Investment ● Trust ● Money lending ● Foreign currency exchange	● Finance leasing ● Credit cards ● Real estate ● Precious metals/stones ● Postal receiving services	● Telephone receiving services ● Telephone forwarding services ● Legal/Accounting services

○ **Low-risk Transactions (Transactions for which simplified CDD is permitted, prescribed in Article 4 of the Ordinance)**

Factors that mitigate risks
1. The source of funds is clear. 2. The customer, etc. is a national or local government. 3. The customer, etc. is limited by laws and regulations, etc. 4. Transactions are supervised by the national government, etc. under laws are regulations. 5. It is difficult to disguise the actual business situation of the company, etc. 6. There is little or no accumulated wealth. 7. The transaction amount is lower than the regulatory threshold. 8. The means for verifying the identity of customers, etc. are secured under laws and regulations, etc.

4. Major Changes In NRA-FUR in Light of Recent Changes in Situations

The 2023 NRA-FUR, like last year, encompasses risk assessments from broad to more specific concepts. It has been updated and enriched based on changes in domestic and international situations and the results of the Fourth Round of Mutual Evaluation of Japan by the FATF.

The main points of the update and enhancement are as follows:

(1) The analysis related to the main offenders of money laundering (Boryokudan, online and telephone fraud groups, crime groups of foreigners in Japan) has been deepened, particularly enriching the content regarding recent criminal circumstances surrounding online and telephone fraud.

(2) In light of the amendment to the Act on Prevention of Transfer of Criminal Proceeds in 2022, which added electronic payment instruments service providers as specified business operators, a risk assessment of 'electronic payment instruments dealt with by electronic payment instruments service providers' was conducted and newly listed as main products and services with recognized risks.

(3) Referencing the FATF statements and reports, the risks associated with transactions involving Myanmar have been described, as well as international trends in ransomware and crypto-assets and the situation surrounding Japan.

Additionally, this NRA-FUR introduces guidelines and other materials prepared and published by competent authorities, etc. to promote AML/CFT measures. It also includes the initiatives taken by competent authorities, industry associations, and specified business operators in connection with AML/CFT measures in 2022.

[Enactment of the FATF Recommendations Compliance Act (Act No. 97 of 2022) in December 2022]
In response to the recommendations received following the publication of The FATF's 4th round of Mutual Evaluation Report of Japan in August 2021, which called for strengthening measures against crypto-assets and enhancing money laundering countermeasures, "Act to Partially Amend the Act on Special Measures Concerning the Asset-Freezing of International Terrorists Conducted by Japan Based on United Nations Security Council Resolution 1267, etc., to Deal with International Transfers of Unlawful Funds" (hereafter referred to as "FATF Recommendations Compliance Act") was enacted in December 2022.
The outline of the FATF Recommendations Compliance Act is as follows:

Table 1: Outline of the FATF Recommendations Compliance Act

Strengthening measures against ML

- **Increase in statutory penalties for money laundering crimes (Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Act)**
  Raising statutory penalties for crimes related to concealing criminal proceeds, drug crime proceeds, etc.
  ➡ Effective from December 29, 2022
- **Revision of the scope of property that can be confiscated as criminal proceeds (Act on Punishment of Organized Crimes)**
  Allowing confiscation even when criminal proceeds are not in the form of real estate, movables, or monetary claims.
  ➡ Effective from December 29, 2022
- **Strengthening of the crimes related to the provision of funds for terrorism (Act on Punishment of Terrorist Financing)**
  Adding acts equivalent to current crimes with the purpose of threatening the public, etc., as per treaty wording and raising statutory penalties.
  ➡ Effective from December 29, 2022
- **Establishment of regulations related to due diligence obligations of legal and accounting professionals (Act on Prevention of Transfer of Criminal Proceeds)**
  Adding transaction purposes, beneficial owners of corporations, etc., to the due diligence items for legal and accounting professionals and setting up regulations related to reporting obligations for suspicious transactions.

➡ To be enforced by a date determined by the Cabinet order by June 2024

Strengthening measures against crypto-assets, etc.

Implementation of the Travel Rule for crypto-assets (Act on Prevention of Transfer of Criminal Proceeds)
Imposing obligations (the Travel Rule) on crypto-assets exchange service providers to notify counterpart operators of customer and counterparty information when transferring crypto-assets, etc.
➡ Effective from June 1, 2023

- **Obligation for crypto-assets exchange service providers to establish mechanisms for asset freezing measures (FEFTA)**
  Imposing obligations on crypto-assets exchange service providers, banks, etc., to establish internal control framework of asset-freezing measures.
  ➡ Effective from April 1, 2024
- **Measures against electronic payment instruments transactions (FEFTA)**
  Strengthening asset freezing measures for transactions between residents and non-residents involving new type of assets such as electronic payment instruments.
  ➡ Crypto-assets: Effective from May 10, 2022; Electronic payment instruments: Effective from June 1, 2023.

Section 1. Risk Assessment Method, etc.

1. FATF Guidance

For risk assessment methods, the NRA refers to the FATF Guidance on risk assessment performed at the country level (National Money Laundering and Terrorist Financing Risk Assessment (February 2013)). 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.

(1) Risk Factors

Risk can be seen as a function of the following three factors:

Threat	A person or group of people, objects, or activities with the potential to cause harm to the state, society, economy, etc. Examples: Criminals, terrorist groups and their facilitators, and their funds, ML/TF activities, etc.
Vulnerability	Things that the threat can exploit or that may support or facilitate the threat. Example: The features of a product or type of service that make them attractive for ML/TF activities, factors that represent weaknesses in AML/CFT systems, etc.
Consequence	The impact or harm that ML/TF may cause to the economy and society Example: The impact on the reputation of a country's financial sector, etc.

(2) Assessment Process

The assessment process can generally be divided into the following three stages:

Identification process (stage 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.
Analysis process (stage II)	Conduct the analysis on the identified risks or risk factors taking into account the nature, likelihood, etc.
Assessment process (stage III)	Determine priorities for addressing the risks.

2. National Risk Assessment of Japan

(1) Assessment Method

Taking into account the FATF Guidance, this assessment uses a wide range of inputs, including the FATF Recommendations and its Interpretive Notes[*1], the measures being taken by AML/CFT stakeholders in accordance with the Act on Prevention of Transfer of Criminal Proceeds, the findings pointed out in the Third and Fourth Round of Mutual Evaluation of Japan, and the information relating to ML cases. The following factors are considered in the analysis:

○ Threat

Example: Offenders, including Boryokudan (Japanese organized crime groups), online and telephone fraud groups, and crime groups of foreigners in Japan, and predicate offences such as theft and fraud that generate criminal proceeds.

○ Vulnerability

Example: Products/services such as deposit/savings accounts, domestic exchange transactions, and transaction types, including non-face-to-face transactions, cash transactions, etc.

○ Consequence

---

*1 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.

Example: Volume of criminal proceeds to be transferred, risks of supporting or facilitating organized crimes, impact on sound economic activities, etc.

Subsequently, we identified risk factors*[1] in terms of transaction types, countries/regions, customer attributes, and products/services.

Thus, we analyzed the risk factors in a multipronged and comprehensive manner in conjunction with a wide range of sources, for example, inherent risks of being misused for ML/TF, information concerning ML cases, STRs, and 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.).

(2) Information Used in the Assessment

For the assessment, a wide range of sources of information were collected while making efforts to promote close collaboration between the relevant ministries and agencies for AML/CFT measures.

The following information is actively used for the assessment:

- ○ Statistics, knowledge, and examples of cases retained by the relevant ministries and agencies;
- ○ Information retained by industry associations, information on domestic and overseas products and services handled by specified business operators, and information on the scales and types of actual transactions; and
- ○ Information on the level of understanding and situation of measures implemented against ML/TF by business operators, etc.

In addition to the above, information provided by the law enforcement agency and information on cleared cases of money laundering and STRs in the past three years have also been analyzed. Furthermore, risks unique to Japan and external risks based on the global trends of predicate offences, money laundering, etc. have also been analyzed by utilizing the information and statistics retained or published by international organizations, including information collected through the exchange of opinions with overseas authorities performed by relevant ministries and agencies during international cooperation activities, documents about risk analysis and guidance on supervision using a risk-based approach published by the FATF, and reports regularly issued by the Financial Stability Institute of the Bank for International Settlement.

*[1] 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 business operators.

Section 2. Environment Surrounding 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.

2. Social Environment

The total population of Japan as of October 1, 2022, was approximately 124.95 million, marking 12 consecutive years of decrease. The ratio of the population aged 65 and over to the total population reached a record high of 29.0%, 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*1 entering Japan in 2022 was approximately 4.2 million. Although this represents a significant increase from the previous year due to the relaxation of border control measures implemented to prevent the spread of COVID-19, it is still about 27 million (approximately 86.5%) less than the number of entrants before the pandemic in 2019. The total number of new arrivals was approximately 3.42 million. As far as the number of new arrivals by nationality and region is concerned, the number of South Koreans was the largest, followed by Taiwanese and Americans. Regarding the purpose of entry (status of residence), the number of Temporary Visitors was the largest, followed by foreigners with the residence statuses of Technical Intern Training and Student, respectively.

The number of foreign residents as of the end of 2022 was approximately 3.08 million, 11.4% more than the previous year. In terms of the number of foreign residents by nationality and region, Chinese*2 was the largest and accounted for 24.8% of the total, followed by Vietnamese and Koreans.

3. Economic Environment

The Japanese economy occupies a vital position in the world economy. The nominal GDP in 2022 (Quarterly Estimates of GDP for Apr.-Jun. 2023 (The Second Preliminary Estimates)) was 557.2 trillion yen, the third-largest economy after the United States and China. In terms of purchasing power parity GDP in 2022, it was the fourth largest globally after China, the United States, and India. The real GDP growth rate in FY2022 was 1.4%. The share of nominal gross value added by economic activity(industry) in 2021 was 1.0% for the primary industry, 26.1% for the secondary industry, and 72.9% for the tertiary industry. Regarding the trade value in 2022, Japan's exports amounted to 98.175 trillion yen, and imports amounted to 118.141 trillion yen. Japan's main export partners were China, the United States, South Korea, etc., and its import partners were China, the United States, Australia, etc.

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*3 of STRs related to the main countries subject to economic sanctions between 2020 and 2022 is as follows:

---

*1 The total number of new entrants and re-entrants. "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 for medium to long-term periods and who have temporarily left Japan and then re-entered.

*2 In this NRA-FUR, "Chinese" does not include "Taiwan," "Hong Kong Special Administrative Region" and "Macao Special Administrative Region," unless otherwise specifically stated.

*3 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 responsible for specified business operators.

Table 2: Annual Number of Notifications of STRs Related to Main Countries under Economic Sanctions

Destination (Origin) Country or Jurisdiction	2020	2021	2022
Iraq	9	9	8
Democratic Republic of the Congo	43	58	70
Sudan	2	4	3
North Korea	1	1	1
Somalia	0	1	1
Libya	1	0	0
Syria	1	2	1
Russia	927	901	917
Belarus	9	21	14
Central African Republic	1	1	0
Yemen	0	4	3
South Sudan	1	0	0
Mali	2	5	2
Haiti	0	3	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 2022, the number of branch offices of major financial institutions[*1] was 37,399 (including 172 overseas branch offices). There were 88,000 ATMs[*2] installed with ease of access to the financial system. Furthermore, 3 of the 30 global systemically important banks (G-SIBs) designated by the Financial Stability Board (FSB) in 2022 were Japanese financial institutions.

In terms of the scale of financial transactions in Japan, the balance of bank deposits at the end of March 2023 was approximately 1,152 trillion yen. As for settlement transactions in 2022, domestic exchange transactions (other banks' transaction volume of exchange) comprised approximately 3,336 trillion yen (approximately 1.9 billion cases), with a daily average of about 14 trillion yen (approximately 7.71 million cases), and the amount of foreign exchange in settled in yen was approximately 5,346 trillion yen (approximately 7.3 million cases), with a daily average of about 22 trillion yen (approximately 30,000 cases).

Looking at the size of the securities market, as of the end of December 2022, the total market capitalization of stocks in Japan was approximately 705 trillion yen. During 2022, the trading value[*3] of listed stocks on the Tokyo Stock Exchange was about 606 trillion yen in the Prime Market, 16 trillion yen in the Standard Market, and 25 trillion yen in the Growth Market.

Regarding cash transactions, Japan has a high number of financial institution branches and ATMs, making it easy to withdraw and deposit cash from bank accounts. Furthermore, the high level of anti-counterfeiting technology in

---

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

*2 The total number of city bank, regional bank, trust bank and second regional bank ATMs was calculated as of the end of September 2022, and the number of Japan Post Bank ATMs was calculated as of the end of March 2022.

*3 The Tokyo Stock Exchange reorganized its market segments into three new categories - Prime Market, Standard Market, and Growth Market - on April 4, 2022. Therefore, the trading amounts for the period from January 4 to April 1, 2022, are not included in the 2022 data.

banknotes, resulting in the minimal circulation of counterfeit bills, contributes to a higher cash circulation situation in Japan compared to other countries. On the other hand, with the rise in the ratio of cashless payments*1 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.

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.

4. Criminal Circumstances

(1) Domestic Crime Situation

(i) Number of Recognized Criminal Offence cases, etc.

Among the indicators measuring Japan's criminal circumstances, the total number of recognized criminal offence cases has consistently decreased since 2003. However, in 2022, there were 601,331 cases, surpassing the post-war record low in 2021 (an increase of 5.8% compared to the previous year), indicating a situation that requires close attention for future trends.

The decrease since 2002, the year with the highest number of recognized criminal offence cases the post-war, was 78.9%.

The total number of cleared cases of criminal offences in 2022 was 250,350, a decrease of 5.3% from the previous year, and the percentage of cleared cases also decreased by 5.0 points to 41.6%.

(ii) Cyber Crimes, etc.*2

In 2022, the situation surrounding cyber threats was extremely serious. This includes an increase in ransomware infection damages, the revelation of cyber-attacks targeting crypto-asset-related businesses and academic figures in Japan, and a sharp increase in online banking fraud cases in the latter half of the year.

(A) Situation of Online Banking Fraud Cases

Although the number of online banking fraud cases had been on a declining trend in terms of both the number of cases and the total amount of financial damages since 2020, there was an increase in 2022 for the first time in three years. The number of incidents was 1,136, and the total amount of damages was approximately 1.5 billion yen, marking increases of 94.5% and 85.2%, respectively, compared to the previous year.

Most of these financial damages are believed to be due to phishing, with a significant number of emails detected that lead to phishing sites masquerading as financial institutions. The Council of Anti-Phishing Japan reported that the number of phishing incidents in 2022 was 968,832, an increase of 84.0% from the previous year, indicating a rising trend. The emails frequently impersonated credit card companies and e-commerce businesses (see Table 3). Additionally, the Japan Consumer Credit Association reported that the damages from credit card fraud due to number theft in 2022 amounted to about 41.2 billion yen, a 32.1% increase from the previous year*3.

---

*1 According to the calculations by the Ministry of Economy, Trade, and Industry, the cashless payment ratio in 2022 increased from 26.8% in 2019 to 36.0%.

*2 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.

*3 "The Japanese Credit Statistics 2022 Edition" on the Japan Consumer Credit Association's website.

Table 3: Number of Reports on Phishing

	2018	2019	2020	2021	2022
Number of reports	19,960	55,787	224,676	526,504	968,832

(B) Situation of Ransomware

In 2022, the number of ransomware attack cases reported to the National Police Agency was 230 cases, a 57.5% increase compared to the previous year, marking a continuous rise since the second half of 2020 (see Table 4). The impact of these incidents is widespread, affecting companies and organizations of all sizes and industries. Notable cases include disruptions in production and sales activities at domestic automobile-related companies and interruptions in the electronic medical record systems of medical institutions, leading to postponed surgeries and temporary suspension of outpatient and emergency services. These incidents have had a significant impact on the functionality of social infrastructure and, consequently, on the lives of citizens and socio-economic activities. Focusing on the infection routes, vulnerabilities in VPN devices remain a common gateway for ransomware infections. Once infected, the damage is not limited to the affected organization, with cases of the infection spreading to businesses involved in the supply chain also being observed.

Key characteristics of victims of ransomware attacks include the following:

○ Many of them were victims of double extortion[*1].

The police were able to figure out the modus operandi used by criminals to demand payment in 182 of all 230 cases of ransomware attacks and 119 cases of those involved double-extortion, accounting for 65%.

○ In many cases, criminals demanded payment in crypto assets.

In 54 cases of all 230 cases, criminals directly demanded payment from victims, and in 50 of those cases, criminals demanded money in crypto-assets, accounting for 93%.

○ Regardless of size, companies, organizations, etc. have become victims of ransomware attacks.

Looking at the cases of ransomware attacks (230 cases) by the size of companies and organizations, etc.[*2], in 63 cases, the victims were large companies. In 121 cases, the victims were small and medium-sized ones. In this way, ransomware attacks caused damage to companies regardless of their size.

Table 4: Number of Reports on Ransomware Attacks Submitted by Companies and Organizations, etc.

	Second half of 2020	First half of 2021	Second half of 2021	First half of 2022	Second half of 2022
Number of reports	21	61	85	114	116

(C) Cyber-attacks Targeting Specific Businesses and Entities

Cyber-attacks that are similar to those used by a group known as Lazarus, which is believed to be under the North Korean authorities, have been carried out against crypto-assets exchange service providers in Japan. For several years now, it has been strongly suspected that this cyber-attack group has targeted Japanese-related businesses. In recent years, numerous cyber-attacks have been confirmed, attempting to steal information by executing malicious programs using common methods against domestic academics and think tank researchers.

---

*1 "Double-extortion" means that criminals demand a ransom (in money or crypto assets) from companies, etc. after encrypting and stealing data from them by saying "the data will be disclosed if payment is not made."

*2 Classified pursuant to Article 2, paragraph 1 of the Small and Medium-Sized Enterprise Basic Act.

(D) Status of Cleared Cases

The number of cleared cases[*1] for cyber crime cases from April to December 2022 was 1,844. Looking at the trend in cybercrime[*2] arrests, which have been increasing in recent years, the number of arrests in 2022 reached a record high of 12,369 (see Table 5).

Table 5: Status of Cybercrime Cleared Cases

	2018	2019	2020	2021	2022
Number of cleared cases	9,040	9,519	9,875	12,209	12,369

Furthermore, the number of arrests for violations of the Unauthorized Computer Access Law in 2022 was 522, an increase of 93 compared to the same period of the previous year. The characteristics are as follows:

- ○ Out of the total arrests, 482 cases were of identity code theft type[*3], accounting for 92.3%.
- ○ The most common method in the identity code theft type of unauthorized access was exploiting weak password settings and management by the rights holder.
- ○ The most frequently exploited services by the suspects were online games and community sites, followed by exclusive sites for employees and members.

(2) Terrorism Situation

As for the international terrorist situation, ISIL*[4] calls on sympathizers to carry out terrorism against Western and other countries participating in the Global Coalition to Counter ISIL. Besides, AQ*[5] and related organizations are also calling to execute terrorism against Western countries, etc. Furthermore, in Afghanistan, where the Taliban took control of Kabul in August 2021, there is growing concern that Islamic extremist organizations based in the country may become more active. Terrorist attacks occurred worldwide, and there were also cases in which Japanese people and the interests of Japan abroad were targeted by terrorism. As such, the threat of terrorism against Japan still exists. Although many years have passed since the abductions by North Korea occurred, not all victims have yet returned to Japan. There is no time to lose before resolving this issue.

In addition to this situation, cyberattacks targeting government agencies and companies are occurring globally in cyberspace. There is, therefore, also a concern that cyber terrorism that will paralyze the society's functions may occur in Japan.

---

*1 Data collection started following the implementation of the amendment to the Police Act (Act No. 6 of 2022).

*2 Violations of the Unauthorized Computer Access Act (Act on Prohibition of Unauthorized Computer Access, Act No. 128 of 1999), crimes targeting computer or electromagnetic records, and other crimes utilizing advanced information and communication networks as essential means for execution.

*3 Unauthorized access activities are classified into two types: Identity Code Theft Type, where unauthorized input of another person's identification code occurs, and Security Hole Attack Type, which involves inputting information (excluding identification codes) or commands to bypass restrictions set by access control functions.

*4 The acronym for the Islamic State in Iraq and the Levant. Commonly known as the Islamic State.

*5 Abbreviation for Al-Qaeda

Section 3. Analysis of Money Laundering Cases, etc.

The number of cleared Money Laundering cases *1 in 2022 was 726, an increase of 94 cases compared to the previous year (see Table 6).

Table 6: Number of Cleared Money Laundering Cases

Category \ Year	2020		2021		2022	
	Number of cases	Percentage (%)	Number of cases	Percentage (%)	Number of cases	Percentage (%)
Number of cleared cases of money laundering offences	600	—	632	—	726	—
Related to the Act on Punishment of Organized Crimes	597	99.5	623	98.6	709	97.7
Related to the Anti-Drug Special Provisions Act	3	0.5	9	1.4	17	2.3

1. Offenders

Although there are various types of perpetrators of money laundering, Boryokudan (Japanese organized-crime groups), online and telephone fraud groups, and criminal groups of foreigners in Japan are considered to be the main offenders.

(1) Boryokudan

In Japan, money laundering by Boryokudan is an especially serious threat. Among cleared money laundering cases in 2022, 64 cases (8.8%) were related to Boryokudan members, associates, and other related parties (hereinafter referred to as "Boryokudan gangsters") (see Table 7). Out of those, 62 cases involved a violation of the Act on Punishment of Organized Crimes (1 case of corporate/business management control, 43 cases of concealment of criminal proceeds, and 18 cases of receipt of criminal proceeds), and 2 cases involved a violation of the Anti-Drug Special Provisions Law (2 cases of concealment of illegal drug proceeds).

In terms of the number of cleared cases of money laundering from 2020 to 2022 in which Boryokudan gangsters were involved in relation to predicate offences, the majority was fraud, theft, and loan sharking*2.

Furthermore, the total amount of criminal proceeds (limited to those that can be monetized) was approximately 1.35 billion yen. As to the form of these criminal proceeds, cash including bank deposits, accounted for 75.8% of the cleared cases, with an average of about 7.3 million yen per case.

When analyzed by transaction type, domestic money transfers*3 accounted for 31.3% of all cases, while 21.6% of cases involved receiving criminal proceeds in cash without involving any goods or services. Looking at the accounts used by Boryokudan gangsters, 82.3% were held in the name of fictitious or other parties, with 31.6% in the name of acquaintances of Boryokudan gangsters and 21.5% in the name of family members, indicating that more than half of the accounts used were in the names of those closely related to Boryokudan gangsters.

Boryokudan repeatedly and continuously commit crimes to gain economic profit, and skillfully engage in money laundering with the gained criminal proceeds.

Money laundering 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*4 imposing economic

*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 Law.

*2 Meaning the cases of unregistered business operation and high interest rate offences (violation of the Money Lending Business Act (Act No. 32 of 1983) (unregistered business operation) as well as the cases of violation of the Investment Act (offences related to (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).

*3 For other transactions, they are described in the section '2 (2) Main Transactions Misused for Money Laundering' under 'Part 3: Analysis of Money Laundering Cases, etc.' in this report.

*4 Executive Order 13581 of July 24, 2011

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.

Table 7: Number of Cleared Money Laundering Cases Committed by Boryokudan Gangsters

Category \ Year	2020		2021		2022	
	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	58	9.7	64	10.1	64	8.8
Related to the Act on Punishment of Organized Crimes	57	9.5	60	9.6	62	8.7
Related to the Anti-Drug Special Provisions Act	1	33.3	4	44.4	2	11.8

(2) Online and telephone fraud[*1] Group

Fraud groups involved in Online and telephone fraud schemes orchestrated by the mastermind, have become more sophisticated by subdividing roles such as so-called "callers," "receivers," "senders," "cash collectors & carriers," "recruiters," "crime tool procurement agents," etc. They use highly secretive communication methods for instructions and coordination between the leaders and the executors. Furthermore, they cleverly misuse various tools, such as deposit/savings accounts, mobile phones, telephone-forwarding services, etc., to commit organized fraud.

Furthermore, there are some people who thoughtlessly sell their own bank accounts or bank accounts opened under the names of fictitious or third parties by using falsified identifications. Such people make it easier for criminals to launder money. In recent years, the existence of foreign crime bases of operation has surfaced, and it has been recognized that criminal proceeds from online and telephone fraud are being transferred abroad.

Moreover, malicious businesses that illegally transfer deposit/savings accounts and mobile phones to fraud groups or provide services like telephone forwarding still exist. There have been cases where telephone-forwarding service providers, knowing their services were being used for online and telephone fraud, provided VoIP services or colluded with online and telephone fraud groups to allow electronic money obtained through online and telephone fraud to be purchased by buyers and then deposited the proceeds into the personal accounts of other telephone-forwarding service providers. This shows that businesses handling services exploited for online and telephone fraud are actively involved in the execution of these frauds.

Within the police force, comprehensive measures have been developed to protect older people from online and telephone fraud, etc. These measures include the "It's me fraud countermeasure plan", which was established in June 2019 at the Ministerial Meeting Concerning Measures against Crime, and the "Emergency measures against robbery and online and telephone fraud cases that involve the recruitment of perpetrators on social media" formulated in March 2023 at the same meeting. Based on these initiatives, efforts are being made to eradicate online and telephone fraud and similar crimes in collaboration with relevant ministries and agencies, business operators, and other stakeholders.

[Recent Situation concerning Crimes Committed by Online and Telephone Fraud Group]
1. Number of Recognized Online and Telephone Fraud Cases, etc.

*1 Online and telephone fraud is the 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.

In 2022, the number of recognized online and telephone fraud cases was 17,570, with the total damage amounting to 37.08 billion yen. These figures represent an increase compared to the previous year, and the amount of damage has increased for the first time in eight years, indicating a serious situation. The damage is concentrated in major urban areas, with recognized cases in Tokyo being 3,218, Kanagawa 2,090, Osaka 2,064, Chiba 1,457, Saitama 1,387, Hyogo 1,074, and Aichi 980, accounting for 69.8% of the total recognized cases in these seven prefectures. Additionally, the proportion of elderly victims (aged 65 and over) in the total number of recognized cases (excluding corporate victims) is 86.6%, with older women aged 65 and over particularly affected, accounting for 66.2% of the victims.

Table 8: Number of Recognized Online and Telephone Fraud Cases & Total Financial Damage

Category \ Year	2020	2021	2022
Number of recognized cases	13,550	14,498	17,570
Total financial damage (yen) (Actual total damage amount)	28,523,359,039	28,199,462,547	37,081,354,580

Note 1: Based on data from the National Police Agency.
2: The actual total damage amount includes the amount withdrawn from ATMs using cash cards that were fraudulently obtained or stolen (calculated based on practical statistics).

2. Modus Operandi of Online and Telephone Fraud

The main methods of online and telephone fraud and the number of recognized cases in 2022 are as follows:

○ "It's me Fraud" (Number of recognized cases: 4,287 (24.4% of total), Damage amount: 12.93 billion yen)
A method where the perpetrator impersonates a family member, police officer, lawyer, etc., and deceives the victim into paying settlement money for an incident or accident allegedly involving a family member.

○ Savings Account Fraud (Number of recognized cases: 2,363 (13.4% of total), Damage amount: 2.89 billion yen)
Impersonating staff from municipalities or tax offices, the perpetrator claims there is a refund due for medical expenses, etc., and visits the victim's home under the pretext of needing to check or replace the cash card, then fraudulently obtains the card.

○The fraudulent theft of cash cards (Number of recognized cases: 3,074 (17.5% of total), Damage amount: 4.69 billion yen)
Posing as a police officer, the perpetrator calls the victim and lies about their bank account being misused or needing to take steps to protect their savings, then explains fake procedures and steals the cash card by switching it with another.

○ Fictitious Fee Request Fraud (Number of recognized cases: 2,922 (16.6% of total), Damage amount: 10.18 billion yen)
This type of fraud involves deceiving people into paying money based on non-existent facts, such as unpaid fees.

○ Refund Fraud (Number of recognized cases: 4,679 (26.6% of total), Damage amount: 5.37 billion yen)
This scam involves tricking victims into operating ATMs under the pretense of necessary procedures for tax refunds, resulting in the perpetrators illegally gaining financial benefits through inter-account transfers.

As mentioned above, when examining the number of recognized cases by type of crime, refund fraud, which surged in 2021, accounts for 26.6% of the total, while other types like "It's me Fraud" and the fraudulent theft of cash cards also constitute a significant proportion.

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 theft, as well as non-face-to-face methods like bank transfers, cash mailing, and electronic money.
The number of recognized cases for each form of payment in 2022 is as follows in the next table.

Table 9: Recognized Cases by Form of Payment

	Payment form	Number of recognized cases	Damage Amount (billion yen)	Proportion of total cases (%)
Face-to-face	Cash handover type	3,981	13	22.7
	Cash card handover type	2,671	3.98	15.2
	Cash card theft type	3,074	4.69	17.5
Non-face-to-face	Transfer type	6,058	10.53	34.5
	Cash mailing type	319	3.86	1.8
	Electronic money type	1,416	0.99	8.1

Note 1: Based on data from the National Police Agency.
2: This does not include the number of recognized cases and damage amounts other than those mentioned

above.

The most common type of fraud by number of recognized cases is the transfer type, where victims are deceived into thinking they are operating an ATM touchscreen to receive a refund in their account. However, in reality, they inadvertently transfer money from their account to one controlled by the criminals. The main destination for these transfers is accounts managed by the crime groups, held in fictitious names or other parties' names, indicating the occurrence of money laundering.

4. Money Laundering Cases

Money laundering cases involving online and telephone fraud groups include, but are not limited to, the following:

- ○ Transferring swindled money into bank accounts under the names of fictitious or other parties and then withdrawing cash.
- ○ After transferring the swindled money into bank accounts under the names of fictitious or other parties, the money is either sent to another bank account or a crypto-assets exchange service account controlled by the criminals.
- ○ Using fraudulently obtained cash cards to operate ATMs, transferring money to bank accounts under the names of fictitious or other parties controlled by the criminals, and then withdrawing cash.
- ○ Using fraudulently obtained cash cards to operate ATMs, transferring money to crypto-assets exchange service accounts, and depositing it into accounts controlled by the criminals.
- ○ Selling 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.

While the stolen money is often received in cash or deposited into bank accounts under the names of fictitious or other parties, there are also cases where electronic money rights (prepaid payment instruments) are illegally obtained. Furthermore, to avoid freezing by financial institutions after the discovery of the crime, the criminals tend to refund immediately, transfer to other accounts, or move the stolen money through multiple accounts after deposit, and sometimes even transfer it to crypto-asset accounts.

The name of accounts used for these transfers vary, including individual names, corporate names, sole proprietorship names, and accounts sold by foreigners when leaving Japan.

5. Communication Methods Used in Online and telephone fraud and Countermeasures

Most online and telephone fraud cases originate from phone calls made by criminals. When the police identify the criminals' phone numbers, they request communication service providers to turn off these numbers to prevent further damage.

It has been observed that some criminals use telephone-forwarding services, and some service providers intentionally provide phone numbers to crime groups, knowing they will be used for crimes. In June 2023, the Ministry of Internal Affairs and Communications revised its scheme to suspend the use of fixed-line phone numbers, etc., owned by malicious telephone-forwarding service providers when certain conditions are met.

The use of application software that enable calls from specific IP phone numbers starting with "050" on mobile devices (such as smartphones and tablets) is also common. Therefore, in August 2023, the Ministry amended a ministerial ordinance to include 050 app phone calls as the service that is be subject to the identity verification obligation at the time-of-service provision contract under the Mobile Phone Improper Use Prevention Act.

6. Efforts Toward Prevention of Damages

Financial institutions promote measures such as speaking to older people at ATM locations and not allowing mobile phone use at ATMs to prevent fraud. In addition, it is important to review and properly adjust the restrictions and standards for ATM transfers and withdrawals based on the customer's transaction history, age, and other information, especially when there is a risk of fraud. Furthermore, at bank counters, even when employees verify the purpose of withdrawals, victims may still follow the criminals' instructions and provide false reasons. Therefore, more thorough responses are necessary when there is a risk of customers being involved in online and telephone fraud or similar crimes. Additionally, individual financial institutions are undertaking measures such as detecting suspicious activities in accounts that may be victims of online and telephone fraud during ATM transactions and preventing withdrawals and transfers from these accounts. As a response to accounts that have been illicitly transferred and used for online and telephone fraud, efforts include strengthening identity verification to prevent account creation through impersonation and monitoring accounts, especially those under foreign nationals' names, to prevent misuse after their residency period has ended.

Online and telephone fraud groups adapt their methods, regions, and times of operation in response to changes in societal conditions. Therefore, countermeasures against online and telephone fraud are a crucial social issue that requires broad collaboration and unified efforts between the public and private sectors.

(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. Such crimes are characterized by the

[*1] "Foreign nationals visiting 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.

fact that their human networks, mode of committing offences, etc., are not limited to one country. This is evident in cases where crime groups consisting of foreigners, etc., in Japan commit crimes following instructions from crime groups existing in their home countries, and these offences tend to be more sophisticated and hidden since the tasks assigned are carried out by different offenders in different countries involved.

Of the cleared money laundering cases in 2022, 108 cases (14.9%) were committed by foreigners in Japan (see Table 10).

Table 10: Number of Cleared-Money Laundering Cases (Committed by Foreigners in Japan)

Category \ Year	2020		2021		2022	
	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	79	13.2	91	14.4	108	14.9
Related to the Act on Punishment of Organized Crimes	79	13.2	91	14.6	103	14.5
Related to the Anti-Drug Special Provisions Act	0	0	0	0	5	29.4

An examination of cleared cases for money laundering offences over the past three years under the Act on Punishment of Organized Crimes by nationality reveals a significant presence of individuals from China and Vietnam, with China accounting for nearly half of all cases. Breaking these down by the type of predicate offenses, fraud is the most common, followed by theft and violations of the Immigration Control Act. In terms of offence the type of transaction, domestic exchange transactions are the most common, followed by credit card transactions, cash transactions, and prepaid payment instruments.

Additionally, in money laundering offences that involve the misuse of domestic exchange transactions and deposit transactions, over 60% use bank accounts under the names of fictitious or other parties with foreigners as the named account holders.

As for the number of criminals arrested for illegal transfers, etc. of deposit books and cash cards, etc., 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. Recently, there has been a remarkable increase in reports related to Vietnamese. Recent trends of crimes committed by foreigners in Japan are as follows:

[Recent Situation Concerning Crimes Committed by Foreigners in Japan]

In 2022, the total number of cleared cases related to crimes committed by foreigners in Japan (both under the Penal Code offences and special law offences) and the total number of offenders arrested (both under the Penal Code and special law offences) decreased compared to the previous year. Additionally, Vietnamese and Chinese accounted for about 60% of the total number of offenders in cleared cases and the total number of offenders arrested, and Vietnamese represented the highest percentage among the total for the second consecutive year. The breakdown of the 9,548 people in 2022 arrested by nationality includes 3,432 Vietnamese (35.9%), 2,006 Chinese (21.0%), 626 Filipinos (6.6%), 509 Brazilians (5.3%), and 348 Thais (3.6%).

The total amount of loss from offences against property by foreigners in Japan arrested in 2022 was about 1.9 billion yen, of which about 1.4 billion yen (73.3%) was from theft, and about 0.5 billion yen (26.2%) was from intellectual crimes.

1. Situation of Crimes Committed by Vietnamese Nationals in Japan

Arrests of Vietnamese in Japan accounted for 41.8% of the total number of cleared cases for crimes by foreigners and 35.9% of the total number of arrested individuals, making them the most arrested nationality. Looking at the types of Penal Code offences committed by Vietnamese nationals, theft accounts for 73.2%, with shoplifting making up 53.8% of these thefts.

There are approximately 490,000 Vietnamese as foreign residents[*1] in Japan, making up about 16% of all foreign residents. Over the past five years, there has been an increase in those entering Japan on Technical Intern Training or Student visas, and some of these individuals have formed criminal organizations through social media platforms. 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. These days, murders have occurred from quarrels among Vietnamese, etc. as well as kidnapping and abduction occurring in connection with borrowing and lending money for gambling.

Looking at the cleared money laundering cases involving Vietnamese in Japan by type of predicate offences, fraud is the most common at 26.9%, followed by theft at 20.5%, and Immigration Control Act violations at 19.2%. Additionally, when looking at the types of transactions misused, domestic exchange transactions are the most common at 28.6%.

Common Examples of cleared cases of money laundering offences committed by Vietnamese in Japan include the following:

- ○ Operating an underground bank by accepting requests for cross-border remittance through social media and depositing cash into bank accounts under the names of fictitious or other parties opened in Japan.
- ○ Depositing sales proceeds from counterfeit residence cards into bank accounts under the names of fictitious or other parties.
- ○ Falsifying the product name and sender on the shipping label when sending stolen cosmetics and other items to disposal agents.
- ○ Using forged residence cards to impersonate fictitious individuals and sell stolen goods.

2. Situation of Crimes Committed by Chinese Nationals in Japan

Arrests of Chinese in Japan accounted for 22.2% of the total number of cleared cases for crimes by foreigners in Japan and 21.0% of the total number of individuals arrested, making them the second most after Vietnam. Looking at the types of Penal Code offences committed by Chinese nationals, theft accounts for 53.0%, fraud for 20.4%, and violent crimes for 13.5%.

There are approximately 760,000 Chinese nationals residing in Japan, constituting about 25% 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, including Chinese nationals, through social media to partake in criminal activities.

Looking at the cleared money laundering cases involving Chinese in Japan by type of predicate offence, theft is the most common at 43.2%, followed by fraud at 36.7%, and computer fraud at 10.8%. When examining the types of misused transactions, credit card misuse is the most common at 25.3%, followed by prepaid payment instruments at 16.0%.

Common Examples of cleared cases of money laundering offences committed by Chinese in Japan include the following:

- ○ An offender received goods that were purchased with unlawfully obtained credit card information by impersonating a card holder.
- ○ 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.
- ○ A restaurant owner stole credit cards from intoxicated customers and made credit card payments, impersonating the cardholder, pretending it was for legitimate food and drink expenses.
- ○ An offender received proceeds from credit card payments at an unlicensed adult-entertainment business by making the payments transferred to a bank account under the name of fictitious or other parties.
- ○ An offender received criminal proceeds obtained through providing a place for prostitution by making the payments transferred to a bank account under the name of fictitious or other parties.
- ○ An offender sold counterfeit goods by using a cash-on-delivery service and made the payments transferred to a bank account under the name of fictitious or other parties to receive criminal proceeds from the sale.

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 a bank account opened in Japan under the name of fictitious or other parties.
- ○ A Burmese national operated an underground bank by accepting requests for cross-border remittance and depositing cash into bank accounts under the name of fictitious or other parties opened in Japan.
- ○ Sri Lankans received compensation for serving as intermediaries for fake marriages by making the payments transferred to a bank account under the name of fictitious or other parties.

---

*1 According to the Immigration Services Agency of Japan's statistics on foreign residents as of the end of December 2022. The term "foreign residents" refers to medium to long-term residents and special permanent residents. The same applies to the rest of this section.

2. Modus Operandi

(1) Predicate Offences

In the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act, 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., using such proceeds are specified as the elements of money laundering offences. 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.

The number of cleared money laundering cases categorized as predicate offences in 2020–2022[*1] is as follows:

Table 11: Numbers and Ratios of Cleared Money Laundering Cases under the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act, Categorized by Predicate Offence

Predicate Offences	Theft	Fraud	Computer fraud	Violation of the Investment Act/ Money Lending Business Act	Habitual gambling/ running a gambling venue for profit	Violation of the Immigration Control and Refugee Recognition Act	Drug-related offences	Violation of the Amusement Business Act	Violation of the Trademark Act	Document forgery offences	Extortion	Distribution of obscene material, etc.	Violation of the Anti-Prostitution Act	Embezzlement	Armed robbery	Unauthorized creation of private electromagnetic records	Others	Total
Number of cases	701	691	220	67	38	34	33	26	26	24	20	20	18	17	13	12	61	2,021
Ratio (%)	34.7	34.2	10.9	3.3	1.9	1.7	1.6	1.3	1.3	1.2	1.0	1.0	0.9	0.8	0.6	0.6	3.0	100

Note 1: Drug-related offences refer to stimulant offences, cannabis offences, narcotics offences, psychotropics offences, and opium offences.
2: Document forgery offences refer to the offences set forth in Articles 154 to 161.1 of the Penal Code.

The size of generated criminal proceeds, relevance to money laundering offences, types of misused transactions, danger of fomenting organized crime, impact on sound economic activities, etc., 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.

(i) Theft

(A) Forms of offences and criminal proceeds

Methods of theft include burglary, vehicle theft, and shoplifting. There are some cases where the amount of financial damage is comparatively small. However, there are also cases in which theft is committed

*1 There were 1,958 cleared cases of money laundering under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Act from 2020 to 2022. On the other hand, the total number of cleared money laundering cases counted by predicate offences was 2,021 (See Table 11) because some money laundering cases can be counted in multiple predicate offences.

continuously and repeatedly by criminal organizations such as Boryokudan and crime groups of foreigners in Japan that result in large amounts of criminal proceeds. The total financial damages from theft during 2022 was about 58.5 billion yen (about 16 billion yen for the total amount of damage in cash), generating a large volume of criminal proceeds.

(B) Money laundering cases

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

- ○ Cases where cash obtained through theft is exchanged by an unsuspecting acquaintance and then further disguised as a transfer from the acquaintance to deposit into an account in the name of the perpetrator.
- ○ Cases that involve purchasing electronic appliances with cash gained from theft and subsequently selling these appliances through a flea market app.
- ○ Cases where an offender used a flea market app to sell stolen goods in fictious or other party's name and made buyers transfer payments to a bank account under the fictious or other party's name.
- ○ Cases of buying and keeping stolen cars knowing that they were stolen.
- ○ Cases where a group of Vietnamese, etc. sent stolen cosmetics and other goods to another offender who disposed of the goods, etc. by lying about the names of goods or name of the sender written on the shipping label.

(ii) Fraud

(A) Forms of offences and criminal proceeds

Frauds, including online and telephone fraud, are repeatedly and continuously committed by domestic and foreign crime groups, generating significant criminal proceeds. In 2022, among property crimes (robbery, extortion, theft, fraud, embezzlement, and misappropriation of lost property), fraud accounted for the highest amount of financial damage, approximately 87.7 billion yen (with about 78 billion yen in financial damages). The average amount of financial damage per case of fraud was about 2.31 million yen, which is higher than the average theft case (about 140,000 yen)

(B) Money laundering cases

Money laundering offences with fraud as the predicate offence include the following cases:

- ○ 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 that involve depositing defrauded money into the perpetrator's account and then using this money to purchase crypto-assets, which are subsequently transferred to a third party's crypto-asset wallet.
- ○ Cases where an offender opened and misused business accounts under the names of shell companies established for receiving criminal proceeds from fraud targeting public benefits.
- ○ 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, loss from fraud offences 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 operate ATMs by using illegally obtained cash cards of others or 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 fictious or others to accounts managed by the offenders. Some of the cash cards used in computer fraud were illegally obtained through online and telephone fraud. Losses due to online banking fraud in 2022 were approximately 1,519.5

million yen.

(B) Money laundering cases

Money laundering 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, etc. belonging to others and transferred money to an account under fictious or other party's name managed by the offenders to allow a Chinese criminal group in Japan to withdraw cash from the account.

○ Cases where an offender illegally used an electronic money payment app that was installed in a smartphone illegally obtained by the offender and added electronic money by making transfers from the bank account linked to the account in the app by impersonating the owner of the smartphone.

○ Cases where, during the application for membership registration in fan clubs online, fraudsters enter stolen credit card information as the payment method for the annual fee, thereby evading payment of the fee.

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

(A) Forms of offences and criminal proceeds

This is loan-shark crime whereby a money lending business operates without a registration and lends money at a high interest rate. Cases include instances of lending without the lender and borrower directly meeting, where the borrower returns money by transferring it to an account under the name of fictious or other party. 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 "buy now, pay later," 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, etc. and collect money from the victims by calling it a payment for the goods. Additionally, there are cases known as 'prepaid purchase monetization,' where a formal sales contract for a product is concluded, and money is lent to the customer 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 2022 exceeded 5.5 billion yen. This indicates that a large amount of criminal proceeds is generated through violations of the Investment Act or Money Lending Business Act.

(B) Money laundering cases

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

○ Cases where debt repayments were remitted to accounts under the name of fictious or other parties to conceal debt repayments to the loan sharks; and

○ 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:

○ Loan sharks required borrowers to send repayments to a post-office box opened under the name of fictious or other party or a fictitious business operator.

○ Loans sharks made borrowers issue bills and/or checks when lending money to the borrowers, and if there was any delay in repayment, the loan sharks brought such bills and/or checks to a financial institution to transfer money to an account under the name of fictious or other party.

○ 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.

(v) Violation of the Immigration Control 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 operatives based in China, various nationalities of residents, including Chinese nationals, were recruited to manufacture forged residence cards within Japan. Since the operatives are located in China, even if manufacturing bases within Japan are exposed and dismantled, they continue to recruit residents, including Chinese nationals, using similar methods and establish new manufacturing bases. Forged residence card offences tend to exhibit a high degree of organization. In 2022, 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

Money laundering offences involving a violation of the Immigration Control 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 an account under fictious or other party's name; and
- ○ 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 in such gambling offences, either directly or indirectly, and gambling is an important source of funds for them.

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 2022, the orders for confiscation were issued against about 3.25 million yen in cash, which was the proceeds from habitual gambling for profit.

(B) Money laundering cases

Money laundering offences involving habitual gambling/running a gambling venue for profit as a predicate offence include the following cases:

- ○ Cases where a gambling offence was committed in an online casino in which money bet by customers had to be paid to an account opened under fictious or other party's name; and
- ○ 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 adult-entertainment businesses or sex-related amusement businesses (hereinafter, "adult-entertainment business, etc.").Criminal proceeds from amusement-related offences are an important source of funds for them. There were cases where foreigners who were staying illegally in Japan worked in the adult-entertainment business, etc., and cases of trafficking in persons where offenders forced victims to engage in prostitution by using violence, intimidation, etc.

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 violation of the Amusement Business Act and the Anti-Prostitution Act. In 2022, there was a case where bank deposit claims of approximately 59.68 million yen, which were the proceeds made in violation of the Amusement Business Act, became subject to order for confiscation.

(B) Money laundering cases

Money laundering offences involving a violation of the Amusement Business Act or the Anti-prostitution Act as a predicate offence include the following cases:

○ Cases where sales proceeds paid with credit cards were transferred to accounts under the name of fictious or other parties.

○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 to receive proceeds made at the unlicensed restaurant; and

○ Cases where a Boryokudan member received criminal proceeds from prostitution through a bank account under the name of a family member.

(viii) Drug-related crimes

(A) Forms of offences and criminal proceeds

Stimulant-related offences account for approximately 50% of all drug-related offences. While the quantity of trafficked stimulant seized in 2022 (289.0 kg) and the quantity of stimulants seized from smuggling (282.1 kg) decreased from the previous year. It can be assumed that smuggling and illicit trafficking of stimulants still generate a large amount of criminal proceeds.

Of the total number of stimulant profit-making offenders arrested (450), the number of Boryokudan gangsters, etc. arrested was 191, accounting for 42.4%. The situation that Boryokudan is deeply involved in smuggling and illicit trafficking of stimulants has continued.

Additionally, cannabis-related offences account for approximately 40% of all drug-related offences, following methamphetamine offences. This percentage has been increasing since 2013, especially among individuals in their twenties and younger age groups. While the seizure of dried cannabis in 2022 (289.6 kg) decreased from the previous year, the seizure of cannabis concentrates for electronic cigarettes (74.0 kg) and the amount seized from smuggling (70.2 kg) saw a significant increase.

The number of Boryokudan gangsters arrested for making profits from cannabis was 105, accounting for 24.1% of the total number of offenders arrested for making profits from cannabis (436). In addition, past research revealed that Boryokudan gangsters, etc., were involved in more than 70% of large-scale cannabis cultivation

for profit. It is admitted that narcotics-related crimes are one of the major sources of funds for Boryokudan gangsters.

Furthermore, evidence gathered in recent years strongly suggests that Boryokudan members collude with overseas drug-related criminal organizations, and is becoming more involved in the distribution of stimulants (from the shipment and import of products to central/intermediate wholesale and distribution to end users in Japan). As for the offshore transaction of stimulant smuggling crimes, in 2019, Boryokudan gangsters and Taiwanese were arrested in a case where about 587 kg was seized. As for overseas drug-related criminal organizations, Chinese, Mexican, and West African drug-related criminal organizations still have a strong presence. Criminal proceeds from drug-related offences are an important source of funds not only for criminal organizations in Japan but also for those based overseas.

When looking at the number of cleared cases for smuggling offences in 2022 by the country or region of origin for stimulants, Malaysia has the highest number, followed by South Africa and Thailand. In contrast, for cannabis, the United States has the highest number, followed by Vietnam and Canada. Furthermore, when examining the foreign nationals arrested for drug trafficking-related offences in 2022 by nationality, for stimulants, Iran and Brazil have the highest numbers, followed by South Korea. For cannabis, Brazil has the highest number, followed by Vietnam and South Korea.

As described above, 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 temporary restraining orders for confiscation before the institution of prosecution prescribed by the Anti-Drug Special Provisions Law in 2022 was 23. The sum of monetary claims subject to the orders was about 25.36 million yen. Besides monetary claims, properties that became subject to temporary restraining orders for confiscation before the institution of prosecution prescribed by the Anti-Drug Special Provisions Law in the past included vehicles, land, buildings, etc., which indicates that criminal proceeds obtained in cash, etc. are transformed into another type of property.

(B) Money laundering cases

Money laundering 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 and
- ○ Cases where an offender had buyers make payments by transfer to a bank account and withdrew cash at an ATM, knowing that the payments were criminal proceeds obtained from the trafficking of cannabis, etc.

In addition to cases where criminal proceeds are deposited into accounts under the name of fictitious or other parties for the purpose of concealing and receiving them, there are also instances of disguising the origin of such funds. This includes exploiting the payment system of online marketplace applications and using funds transfer services to send criminal proceeds obtained from drug smuggling abroad.

[Money Laundering etc. related to Ransomware[*1]]

1. About the FATF Report[*2]

FATF, in its report published in March 2023, highlights the following regarding the characteristics and measures related to ransomware:

(1) Current Situation and Characteristics of Ransomware

- Transactions associated with ransomware attacks have rapidly expanded on a global scale in recent years, leading to an increase in money laundering related to ransomware.
- The ransom payments demanded in 2020 and 2021 are estimated to be up to four times higher compared to 2019.
- Due to technological advancements, the profitability and success rate of attacks have increased significantly. Apart from cases targeting large and significant organizations, there also exists a service-oriented aspect where ransomware attackers affiliate (partner) with user-friendly software kits, known as Ransomware-as-a-Service (RaaS)[*3].
- The impact of ransomware attacks is highly severe, causing damage and disruption to critical infrastructure and services, posing a potential national security threat. The ransomware threat is likely to continue expanding.
- As a result of investigations, it has become evident that ransomware attacks are underreported due to reasons such as the difficulty in detection by private companies, adverse effects on victims' businesses, and concerns about retaliation from attackers.
- The regions targeted by ransomware attackers are primarily North America (52%), followed by Europe (28%), Asia-Pacific (10%), Latin America (6%), and the Middle East/Africa (4%).
- Over half of the victims come from the government sector, public sector, healthcare, industrial products, and services. In recent years, energy, finance, telecommunications, and educational institutions have also become targets.
- Third parties that act on behalf of victims for actions such as ransom payments include incident response companies and insurance companies.

(2) Characteristics of ML/LF related to Ransomware

- Most ransom payments and subsequent money laundering related to ransomware occur through crypto-assets, with crypto-asset exchanges being commonly used.
- Ransomware attackers leverage the international nature of crypto-assets 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 crypto-assets, mixers, and other technologies/methods/tokens that enhance anonymity in money laundering.
- Ransomware attackers often use non-hosted wallets like Unhosted Wallets*[4] and wallets of crypto-assets 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 wallet addresses for each attack.
- Many ransomware networks are connected to countries or regions with a high risk of money laundering, and they deposit or cash out their earnings in such countries or regions.

(3) Measures Required in Each Country

FATF has called for the following actions from each country and region as part of their efforts to combat ransomware attacks and related money laundering:

- Criminalize money laundering related to ransomware.
- Identify and assess the money laundering risk associated with ransomware and take measures to mitigate it.
- Encourage the private sector, including crypto-assets exchange service providers, to STRs and implement appropriate preventive measures.
- Enable law enforcement agencies to investigate, track, and confiscate criminal proceeds related to ransomware.
- Strengthen international cooperation.

---

*1 The situation of ransomware in Japan is described in *4. Criminal Circumstances* under *Section 2. Environment Surrounding Japan* in the NRA-FUR.

*2 Countering Ransomware Financing (March 2023)

*3 Raas (Ransomware as a Service) refers to a criminal business model where ransomware attack elements, such as providing ransomware software kits on the dark web, distributing malware, initial network infiltration into victims' systems, data leakage, and negotiating compensation in lieu of affiliates, are outsourced to external parties, and a certain percentage of fees or compensation is paid as remuneration.

*4 A wallet (account) that is not hosted (managed) by a business entity.

2. Key Focus Points When Submit 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

(2) Major Transactions, etc. Misused for Money Laundering

We analyzed cleared cases of money laundering (3 years from 2020 to 2022) and counted the detected transactions, etc. to be misused for money laundering while conducting criminal investigations [*1] that are presented in Table 12.

Table 12: Major Transactions, etc. Misused for Money Laundering

Year \ Misused transactions	Domestic exchange transactions	Cash transactions	Deposit transactions	Credit card	Prepaid payment instruments (Note1,2)	Crypto assets	Legal persons	International transaction (such as foreign exchanges)	Funds transfer services	Precious metals and stones	Legal/accounting professionals	Foreign Currency Exchanges	Financial instruments	Total
2020	110	120	96	20	11	32	14	16	1	2	1	1	0	424
2021	208	72	40	40	21	9	16	9	9	2	1	1	2	430
2022	266	105	24	55	39	16	6	7	10	1	1	0	0	530
Total	584	297	160	115	71	57	36	32	20	5	3	2	2	1,384

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 2020 and 2021 include transactions that corresponded to prepaid payment instruments within electronic money.

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

- ○ There were 584 cases of domestic exchange transactions[*2], followed by 297 cases of cash transactions and 160 cases of deposit transactions, with the majority of transactions misused for money laundering involving products and services offered by deposit-taking financial institutions.
- ○ There are many cases where those who plan to conduct money laundering 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.
- ○ With the increase in fraudulent use of credit cards, the number of cases where credit cards were misused for money laundering has also risen.
- ○ There is an observable expansion in the misuse of various payment methods, including credit cards, prepaid payment instruments, crypto-assets, and funds transfer services, reflecting the diversification of payment methods.

---

*1 This NRA-FUR takes transactions misused for concealing/receiving criminal proceeds, plus transactions utilized for transforming criminal proceeds, as targets for analysis.

*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.

3. Suspicious Transaction Report (STR)

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators (excluding lawyers, judicial scriveners, certified administrative procedures legal specialists, certified public accountants, and certified tax accountants[*1]) to submit STRs to competent authorities if assets received in specified business affairs[*2] are suspected of being criminal proceeds, or if a customer, etc. engages in money laundering 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.

Looking at the number of STRs reported in 2022 by business type, the percentage of STRs reported by banks and other deposit-taking institutions was the largest, accounting for 74.7% (435,728) of the total STRs, followed by money-lending companies at 7.8% (45,684) and credit card companies at 7.0% (41,106) (see Table 13).

Furthermore, the number of STRs used for the investigation, etc. by the prefectural police in 2022 was 373,849 (see Table 14).

The National Public Safety Commission and National Police Agency collect, organize and analyze the STRs and provide investigative organizations, etc. other than the prefectural police [*3] as well with those that are considered to be useful for investigating money laundering offences or their predicate offences to enable the organizations to use them for secret investigations, criminal investigations and investigations into tax offences, etc.

---

*1 With the amendment of the Act on Prevention of Transfer of Criminal Proceeds, pursuant to the FATF Recommendation Compliance Act, which was promulgated in December 2022, administrative scriveners, certified public accountants, and tax accountants are now required to report STRs, except for matters related to confidentiality obligations. Regarding this amendment, it is stipulated that it will come into effect within a period not exceeding one year and six months from the date prescribed by Cabinet Order, starting from the day of promulgation.

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

*3 Meaning the investigative organizations, etc. set forth in Article 13, paragraph 1 of the Act on Prevention of Transfer of Criminal Proceeds.

Table 13: Annual Reported Number of STRs by Business Type

Category \ Year	2020	2021	2022
	Number of reports	Number of reports	Number of reports
Financial institutions, etc.	402,868	495,029	542,003
Deposit-taking institutions	342,226	411,683	435,728
Banks, etc.	319,812	390,381	414,651
Shinkin Banks, Credit Cooperative	19,793	18,461	18,520
Labour Banks	300	318	316
Norinchukin Banks, etc.	2,321	2,523	2,241
Insurance Companies	2,635	3,458	3,939
Financial Instruments Business Operators	17,933	19,718	19,032
Money Lenders	25,255	35,442	45,684
Funds Transfer Service Providers	6,040	10,499	20,271
Crypto-assets Exchange Service Providers	8,023	13,540	16,550
Commodity Derivatives Business Operators	320	388	318
Currency Exchange Operators	252	201	430
Electronic Monetary Claim Recording Institutions	5	7	0
Others	179	93	51
Financial Leasing Operators	123	163	71
Credit Card Operators	29,138	34,904	41,106
Real Estate Brokers	7	4	11
Dealers in Precious Metals and Stones	63	48	124
Postal Receiving Service Providers	2	0	1
Telephone Receiving Service Providers	0	0	0
Telephone Forwarding Service Providers	1	2	1
Total	432,202	530,150	583,317

Table 14: Number of STRs Used for Investigative Purposes, etc.

	2020	2021	2022
Number of STRs used for investigation	325,643	353,832	373,849

[Examples of Cleared Cases Detected through STRs by the Prefectural Police]

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

1. Cases of Violating the Act on Punishment of Organized Crimes and Other Offences

(1) Deposit-taking institution submitted STRs concerning accounts of foreigners and companies for the following reasons such as:

- ○ There was a request for a refund due to fraud from the remitter concerning inward remittances from abroad.
- ○ In the case of accounts that had not been active for an extended period, there were sudden small cash deposits followed by substantial transfers from multiple financial institutions.
- ○ Large sums of money were received from multiple individuals and specific corporations, and the entire amount was withdrawn on the same day from ATMs.
- ○ There was inconsistency in the explanations provided during the application process for substantial cash withdrawals.
- ○ Information was provided by the remitter indicating that the account was being used for international fraud-related transactions.

Based on STRs as mentioned above, it was discovered that the same account was being used in international fraud cases involving the use of social networking services. Consequently, the account user was arrested under the Act on Punishment of Organized Crimes (concealment of criminal proceeds) and other relevant offences.

(2) Deposit-taking institutions and crypto-assets exchange service providers submitted STRs concerning accounts of Japanese people, foreigners and companies (including those that were declined) for the following reasons such as:

- ○ It was discovered that the account holder was associated with individuals involved in fraudulent activities, and multiple transfers were observed in that account.
- ○ Although an application for opening a corporate account was accepted, there were suspicions of ties with persons affiliated with Boryokudan based on the submitted documents.
- ○ Same-day crypto-asset purchases and withdrawals of equivalent amounts followed significant deposits that deviated from customer information (financial assets).
- ○ IP address sharing was identified between foreign customers with a history of suspicious transactions.
- ○ Logins from physically challenging locations within proximity in time were detected, raising suspicions of impersonation etc.
- ○ It was revealed that large sums of cash were deposited at ATMs, and funds were subsequently transferred abroad through specific foreign accounts or crypto-assets exchange service.

Based on STRs as mentioned above, it was discovered that the account holders had exchanged online and telephone fraud proceeds for crypto-assets and transferring funds abroad. Consequently, the account holders were arrested under the Act on Punishment of Organized Crimes (receipt of criminal proceeds, etc.) .

2. Fraud Cases

(1) Deposit-taking institutions submitted STRs concerning accounts of Japanese people for the following reasons such as:

- ○ It was observed that after making small cash deposits at ATMs located far from their registered address, they would immediately withdraw the funds and frequently check their remaining balance.
- ○ Analysis of security camera images at ATMs revealed that multiple individuals were using the same account.
- ○ Following cash deposits at ATMs located in convenience stores, almost the entire amount would be withdrawn at other locations, leaving no funds in the account.
- ○ After receiving transfers from individuals with unknown relationships, they would withdraw the entire amount on the same day.

Based on STRs as mentioned above, it was discovered that the account holders (associated with Boryokudan) were engaged in organized online and telephone fraud schemes under the guise of refund payments. Consequently, these individuals were arrested on charges of computer fraud and related offences.

(2) Deposit-taking institutions submitted STRs concerning accounts of Japanese people (including those that were declined) for the following reasons such as:

- ○ Through investigation, it was determined that the account holder was a Boryokudan.
- ○ The stated reason for visiting the bank was an unnatural request for a change in the reading and pronunciation of their name, raising suspicions of a change to a fictitious name.
- ○ A case of fraud was notified by a victim.

Based on STRs as mentioned above, it was discovered that the account holder (a member of Boryokudan) had been fraudulently receiving public assistance benefits while concealing their affiliation with the Boryokudan. Consequently, this individual was arrested on charges of fraud.

3. Cases of Violation of the Investment Act and Violation of the Money Lending Business Act

(1) A deposit-taking institution submitted STRs concerning accounts of foreigners (including those that were declined) for the following reasons such as:

- ○ Despite being a technical intern, the account holder received significant and frequent transfers from numerous foreign individuals with unclear relationships. Furthermore, they transferred funds to an unspecified number of foreign individuals, including those whose accounts had been suspended, using the same funds as their source.
- ○ Despite exceeding their permitted stay period, the account holder continued to use ATMs and engage in online transactions. Additionally, there were no updates to their customer information (period of stay).
- ○ Transactions showed consistent and nearly identical deposit and withdrawal amounts over a specific period, with

almost the entire amount being withdrawn from ATMs immediately after deposits, resulting in a consistently low account balance.

○ There were applications for new account openings from individuals with suspicions of previous account freezes.

Based on STRs as mentioned above, it was discovered that the account holder was operating an unregistered lending business targeting foreigners. Consequently, this individual was arrested for violation of the Money Lending Business Act (unregistered operation).

(2) Deposit-taking institutions and crypto-assets exchange service providers submitted STRs concerning accounts of Japanese people, foreigners and companies (including those that were declined) for the following reasons such as:

○ Sudden and significant increases in account balances at the end of the month, followed by nearly complete withdrawals from ATMs on the same day.

○ Despite claiming to be employed, the account holder continued to engage in transactions involving immediate withdrawals of transfers from multiple third parties, including fixed individuals, which appeared unusual based on the customer's profile.

○ Repeated transfers to numerous individuals, including foreigners, using transfers from multiple foreign sources as the source of funds. Despite conducting transactions on a business scale, there was no confirmation of the account holder's actual business activities.

○ Continuously engaging in transactions involving amounts that are generally round figures, following withdrawals of transfers from numerous individuals with unclear relationships.

○ Transactions involve Boryokudan or persons affiliated with Boryokudan, etc.

Based on STRs as mentioned above, it was discovered that some of the accounts were being used for organized illegal lending activities. Multiple individuals involved, including the account holders (Boryokudan-related individuals), were arrested on charges of violation of the Money Lending Business Act (unregistered operation) and violation of the Investment Law (excessive interest rates).

4. Narcotics-Related Crimes

(1) Deposit-taking institutions and fund transfer service providers submitted STRs concerning accounts of Japanese people for the following reasons such as:

○ Visitors to the bank were observed making cross-border remittance requests while receiving instructions from companions, displaying unsettled behavior, and raising suspicions.

○ On the same day, funds were being transferred to countries deemed to have a high risk of illicit remittances.

○ Unusual cross-border remittance requests were made without reasonable justification.

Based on STRs as mentioned above, it was discovered that multiple individuals, including the account holders, were involved in smuggling narcotics (specifically stimulants) into the country from abroad. Consequently, these individuals were arrested for violating the Anti-Drug Special Provisions Act (possession in concert).

(2) Deposit-taking institutions submitted STRs concerning accounts of Japanese people (including those that were declined) for the following reasons such as:

○ Multiple instances of round-figure transfers from various unidentified individuals, followed by nearly complete withdrawals of these amounts on the same day.

○ Despite being a recipient of public welfare assistance, the account holder received deposits from numerous unidentified individuals into their welfare payment account.

○ Transactions involve Boryokudan or persons affiliated with Boryokudan, etc.

○ An account holder is on the list of account holders subject to account-freezing orders.

Based on STRs as mentioned above, it was discovered that questionable fund movements were associated with the same account. Consequently, multiple individuals related to the account holder (persons affiliated with Boryokudan) were arrested for violating the Stimulants Control Act (possession for profit).

5. Case of Violation of the Immigration Control Act

Deposit-taking institutions submitted STRs concerning accounts of Japanese people for the following reasons such as:

○ Frequent and rapid transactions were observed over a short period, with nearly consistent deposit and withdrawal amounts over a specific timeframe.

○ Repetitive transfers to numerous individuals, including foreigners, with unclear relationships between the sender and recipient, as well as uncertain purposes for the transfers.

○ Unusual transactions that deviated from previous transaction patterns.

○ Multiple transactions were identified with individuals suspected to be associated with organized crime (Boryokudan-related individuals), involving continuous same-day withdrawals and fund transfers.

Based on STRs as mentioned above, it was discovered that the account holder had received intermediation services from individuals associated with organized crime (persons affiliated with Boryokudan) and had engaged foreign individuals in unlawful employment activities. Consequently, this individual was arrested for violating immigration laws (aiding unlawful employment).

6. Case of Violating the Trademark Act

Deposit-taking institutions submitted STRs concerning accounts of Japanese people and foreigners for the following reasons such as:

○ Sudden transfers from a flea market app to an account that had been inactive for a while, with almost the entire amount being withdrawn within a few days.

○ Transferring funds from multiple flea market apps to individuals with unclear relationships via internet banking, where the transaction activity deviated from the intended use of the account.

○ Confirmation of a different individual using the account through security camera images at ATMs and further discovery that this person was using multiple accounts under different names.
○ Information provided by the flea market app operators about allegations of trademark infringement by trademark rights holders.

Based on STRs as mentioned above, it was discovered that the account holder had been selling counterfeit goods using multiple free marketplace apps. Consequently, this individual was arrested for violating the Trademark Act.

7. Case of Violating the Act on Prevention of Transfer of Criminal Proceeds

Deposit-taking institutions and crypto-assets exchange service providers submitted STRs concerning accounts of Japanese people for the following reasons such as:

○ Numerous transfers from unidentified individuals on the same day.
○ Frequent transfer transactions with numerous individuals, including specific individuals, followed by immediate cash withdrawals on the same day.
○ Deposits within a short time frame from multiple physically distant locations, with third-party usage confirmed through verification of the account holder's identity.
○ An account holder is on the list of account holders subject to account-freezing orders.

Based on STRs as mentioned above, it was discovered that the account holder had transferred multiple pieces of crypto-assets exchange information (login IDs and passwords) to third parties. Consequently, this individual was arrested for violating the Act on Prevention of Transfer of Criminal Proceeds (commercial transfer of crypto-assets exchange information).

8. Case of Violating the Banking Act (Underground Banking)

Deposit-taking institutions and crypto-assets exchange service providers submitted STRs concerning accounts of foreigners for the following reasons such as:

○ Despite being an international student, the account holder repeatedly engaged in transactions involving transfers of funds from numerous individuals with unclear relationships to third parties, which appeared unnatural based on the customer's profile.
○ Suspicion arose due to receiving significant transfers from numerous foreigners and subsequently transferring funds to crypto-assets exchange service providers.
○ Transactions involved the immediate conversion of Japanese yen into crypto assets after deposit, followed by repeated overseas transfers.
○ Despite exceeding the permitted stay period, ATM transactions and other activities continued without updating customer information (period of stay).
○ Confirmation through security camera images at ATMs revealed the use of accounts held under different names at other financial institutions.

Based on STRs as mentioned above, it was discovered that multiple individuals using the same account were systematically engaging in unlicensed banking activities. Consequently, these individuals were arrested for violating the Banking Act (Act No. 59 of 1981).

9. Case of Indecent Electronic Record Transmission and Distribution Incident

Deposit-taking institutions submitted STRs concerning accounts of Japanese people for the following reasons such as:

○ Funds were received through a foreign financial institution from an adult website operating company as advertising fees.
○ Repeated high-value remittances were received from overseas.

Based on STRs as mentioned above, it was discovered that multiple individuals, including the account holder, were selling video files containing indecent acts recorded through the use of internet-based video sales platforms. Consequently, these individuals were arrested for the transmission and distribution of indecent electronic records.

[Examples of Cases in Which Investigative Organizations, etc. Other than the Prefectural Police Utilized STRs]

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

1. Public Prosecutors Office

Deposit-taking institutions submitted STRs concerning accounts of Japanese people for the following reasons such as:

- ○ Total amount of funds transferred to another bank, using cash deposits as the source was substantial.
- ○ A large amount of cash from unidentified sources were deposited at ATMs and repeatedly transferred funds through internet banking.
- ○ An account holder did not disclose information on sources of funds for remittances and provided inconsistent explanation about the transaction details made about in response to inquiries large remittances.

By utilizing the STRs submitted for the above reasons, the Public Prosecutors Office arrested suspects on charges of in Embezzlement in the Pursuit of Social Activities cases.

2. National Tax Agency

Deposit-taking institutions submitted STRs concerning accounts of Japanese people for the following reasons such as:

- ○ A large amount of cash was deposited at ATMs, and the funds were repeatedly transferred to multiple individuals and companies;
- ○ For deposit and withdrawal by individuals, relatively large amount of money was moved; and
- ○ When they withdrew a great deal of cash at bank counters, they did not give any clear answers to questions about the purpose of the withdrawal and showed suspicious behavior including talking on the mobile phone restlessly while waiting.

By utilizing the STRs submitted for the above reasons, the National Tax Agency accused cases for violating the Corporation Tax Act, etc. and violation of the Consumption Tax Act, etc.

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

- ○ In 2022, the National Tax Agency accused cases for illegal receipt of refund of consumption taxes (a case where a corporation running a sales outlet of export items abused the tax-free export system by recording fictitious tax-free sales to foreign tourists and a case where multiple corporations used a fraudulent scheme in which fictitious taxable purchases were recorded), non-filing cases (a case of a sole business proprietor selling information on boat racing prediction through websites) and large-scale international cases (a case where fictitious commission fees for payment to foreign entities were recorded and a case where a subject involving in domestic transactions of crypt assets was disguised as a foreign corporation). In addition, National Tax Agency accused cases to achieve substantial spillover effects on the society; a case related to sales business of trading card whose market is expanding in recent years, a case where guidance for fraudulent refund of income taxes was provided to many salary earners through social media, etc., and cases involving employees of main contractors who concealed funds received from subcontractors as their income, etc. Looking at accused cases by their type of business, cases involving construction business or real estate business have been ranked high in number.
- ○ Most of the illegal funds obtained through tax evasion is retained in the form of cash or bank deposits. In some cases, however, such illegal funds were used to purchase real estate, luxury cars or watches, to invest in securities, etc., or to pay expenses for amusement such as gambling including horse racing and expensive night clubs.

3. Japan Customs

Deposit-taking institutions submitted STRs concerning accounts of Japanese people and foreigners for the following reasons such as:

- ○ Large amounts of funds were frequently sent from many people who do not have a specific relationship with an account holder.
- ○ Repeated transactions involving numerous foreigners with immediate cash withdrawals on the same day.
- ○ 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.
- ○ Funds deposited by an individual having an account at a different bank were withdrawn immediately after depositing.

The STRs submitted for the above reasons, etc. were utilized to find persons involved in illegal drug smuggling cases, etc.

4. Narcotics Control Department, Regional Bureaus of Health and Welfare, Ministry of Health, Labour and Welfare

Deposit-taking institutions and credit card operators submitted STRs concerning accounts of Japanese people for the following reasons such as:

- ○ A request was made for a copy of an account holder's certificate of residence. However, the certificate of residence did not exist, and a false declaration was suspected.
- ○ Immediate withdrawals were made from remote ATMs shortly after receiving incoming transfers.
- ○ Transactions included round-figure transfers from unspecified individuals under various aliases, often posing as transactions related to flea market app payments or loan repayments
- ○ Repetitive incoming and outgoing transfers were observed with several specific individuals, with changes in the requester's name during the transactions.

*1 These are introduced based on information provided by each investigative organization, etc.

○ Frequent cash deposits and withdrawals were made at ATMs, deviating from the account's historical usage patterns. Security cameras installed at ATMs revealed a discrepancy between the account holder's gender and that of the ATM user.

By utilizing the STRs submitted for the above reasons, etc., the Narcotics Control Department arrested criminals involved in narcotics and stimulant trafficking cases, etc.

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

○ In many cases, bank accounts under the names of fictitious or other parties are used to receive and conceal criminal proceeds from drugs. These accounts may include those acquired through online purchases, obtained from customers purchasing controlled substances, or established under fictitious names. In the initial stages of illicit drug trafficking, there is a strong tendency to use accounts belonging to individuals directly involved in the drug trafficking or their associates. As drug trafficking operations become more prolonged, individuals tend to acquire accounts from customers rather than direct payments, frequently using these accounts under the name of other parties. In some cases, multiple accounts may also be used. In addition, there is a tendency to use accounts of relatives, friends, or acquaintances of drug trafficking group members to aggregate the proceeds from drug trafficking. There have been cases where multiple members of the group hold passbooks and cash cards for the same account, allowing them to use the same account. Furthermore, when financial institutions make inquiries about the intended use of the accounts, they often claim to use online auction sites or flea market apps to avoid suspicion of receiving unnatural transfers from several individuals.

○ Initially, lower-level drug traffickers in the group use their accounts to receive drug payments. However, as new drug traffickers join or other factors come into play, these drug traffickers may gain higher status and shift to using accounts in the names of the newcomers. In such cases, the financial institutions where the accounts are opened may also change. There are also instances where multiple STRs are submitted from specific regions or locations (such as housing complexes).

○ Notable characteristics of transfers include a large number of cash transfers with round-figure from individuals all over the country. In drug trafficking targeted at end users, the transfer amounts tend to concentrate around 10,000 to 30,000 yen. In addition, customers are instructed to use the name of an online auction site or similar when making the transfer, concealing the fact that it is payment for controlled substances. After the funds are deposited, they are often withdrawn on the same day.

○ When purchasing illegal drugs from overseas drug sales websites, crypto assets are often specified as the payment method. In many cases, funds are transferred from self-named accounts in Japanese crypto-asset exchanges to self-named accounts in overseas crypto-asset exchanges. Then, the drug payments are made from there. There have also been cases where overseas postal receiving and forwarding service providers were registered as the destination, and drugs were shipped to Japan through intermediaries who were unaware of the circumstances. Therefore, transactions involving the use of overseas crypto-asset exchanges and similar services that cannot be justified based on their attributes are associated with ML/TF risks.

5. Japan Coast Guard

Deposit-taking institutions submitted STRs concerning accounts of Japanese people for the following reasons such as:

○ The number of deposit and withdrawal transactions at ATMs increased rapidly or otherwise transactions that deviate from the past transactions were made.

○ An account holder frequently engaged in fund transfers or cash deposits at ATMs within a short period, with the total transaction amounts remaining relatively consistent.

○ An account holder suspiciously deposited funds at an ATM and withdrew the funds at an ATM that is far away.

○ An account holder sent remittances to numerous individuals, including members or associates of criminal organizations (Boryokudan).

STRs submitted for the above reasons were utilized to understand the actual circumstances of poaching organizations and their correlations with persons concerned, etc.

[Recent Criminal 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, and cases of poached products being disguised as legitimate products. Poaching has become more invisible and sophisticated.

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

1. Transaction Types

By referring to cleared cases in which foreigners visiting Japan committed money laundering offences, as well as situations that increase the risks of ML/TF (non-face-to-face transactions, cash-intensive businesses, etc.) as described in the FATF's Interpretive Notes to the FATF Recommendations, we identified: (1) non-face-to-face transactions; (2) cash transactions; and (3) cross-border transactions as transactions that affect the level of risk in transactions. We then analyzed and assessed such transactions.

(1) Non-Face-to-face Transactions

(i) Factors that Increase Risks

(A) Characteristics

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 through the Internet. Additionally, there are mail-order services where application procedures for account opening and other services can be completed through postal mail. Furthermore, in the case of financial instruments business operators, account openings and stock trading are conducted through the Internet. There are also specified business operators, like crypto-assets 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. Direct verification of personal identification documents, gender, appearance, behavior, etc., is not possible, making it challenging to detect forged identification documents, misrepresentation of personal details, impersonation of others, or suspicious aspects of transactions. Consequently, the means to detect those planning criminal activities are limited, and it becomes easier for them to falsify their personal identification details or impersonate others.

(B) Typologies

From 2020 through 2022, the main cases of non-face-to-face transactions being misused for money laundering include the following:

- ○ A criminal sent criminal proceeds from fraud to an account for crypto-asset transactions through an online non-face-to-face transaction and purchased crypto-assets.
- ○ 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.
- ○ A criminal sold criminal proceeds from theft on a flea market app and had buyers transfer payments to an account under fictious or other party's name through a non-face-to-face transaction.
- ○ A criminal listed illegally duplicated goods on an internet auction site under fictitious names, and received a payment was collected through non-face-to-face transactions using a payment management service on the site.

(ii)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 completing identity verification online (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 mitigating risks by accumulating knowledge on the characteristics of forged documents and utilizing AI for image analysis. They also check for suspicious details in reported information, such as addresses corresponding to vacant houses or phone numbers used for multiple account openings.

Additionally, 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 for users to falsify personal identification details or impersonate others. Therefore, discussions with industry associations are underway to and promote the use of this method.

Furthermore, to detect unauthorized transactions by third parties, 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.

In the Financial Services Agency’s Guidelines for Supervision provide that one area of focus for supervision is whether financial institutions have developed a system necessary to conduct identity verification at the time of transaction and implementation of other CDD measures based on the fact that online banking is a non-face-to-face transaction.

(iii) 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, etc.

Actually, there are cases where non-face-to-face transactions have been misused for money laundering, including a case where bank accounts opened by pretending to be other person or accounts 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) Characteristics

In 2019, the average monthly consumption expenditure per household (total households) was 174,237 yen in cash (including account debits, etc., same hereafter), which accounted for 73.5% of the total expenditure. In contrast, credit card, installment payments, and credit purchases amounted to 53,305 yen, representing 22.5% of the total. The trend in the proportion of cash was 82.4% in 2014 and 73.5% in 2019, indicating that cash still constitutes the majority of consumption expenditure (see Table 15). However, the proportion of cash used in transactions is showing a decreasing trend due to the spread of cashless payments. On the other hand, the balance of cash in circulation remains high compared to other countries (see Table 16). The issuance volume of high-denomination banknotes (10,000 yen notes) is increasing (see Table 17).

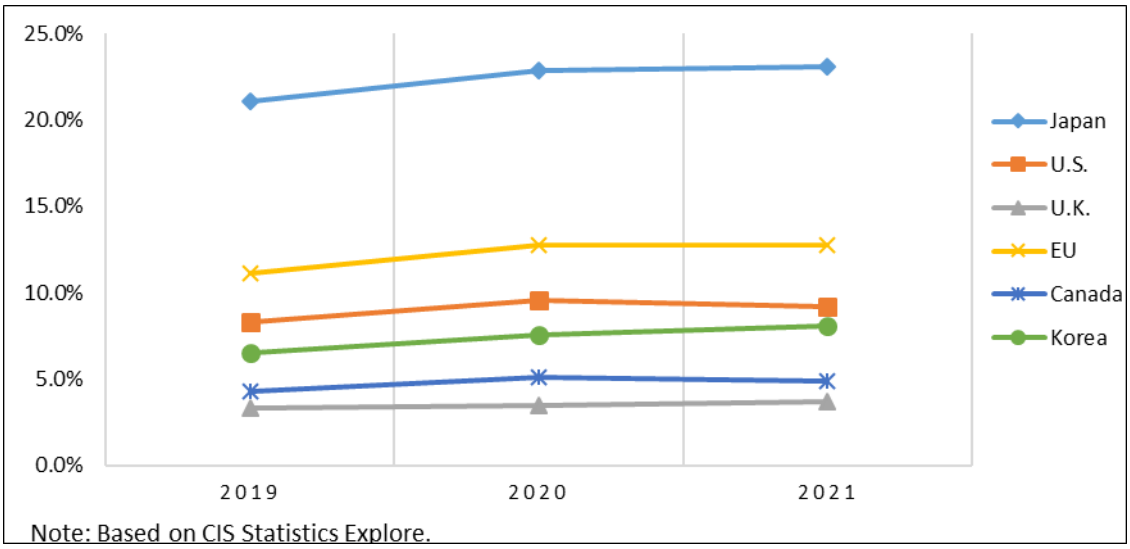
While a reasonable time is necessary for cash transactions because cash is physically transferred, cash transactions are highly anonymous, which is different from foreign/domestic exchange transactions where funds can be transferred to remote locations promptly. Cash transactions are unique in that the 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.

Table 15: Expenditure by Type of Purchase (Total Household/Monthly Average)

Consumption expenditure	2014				2019			
	Cash	Credit card, etc.	Electronic money (prepaid)	Total	Cash	Credit card, etc.	Electronic money (prepaid)	Total
Expenditure amount (yen)	205,846	40,104	3,788	249,738	174,237	53,305	9,550	237,091
Ratio (%)	82.4	16.1	1.5	100.0	73.5	22.5	4.0	100.0

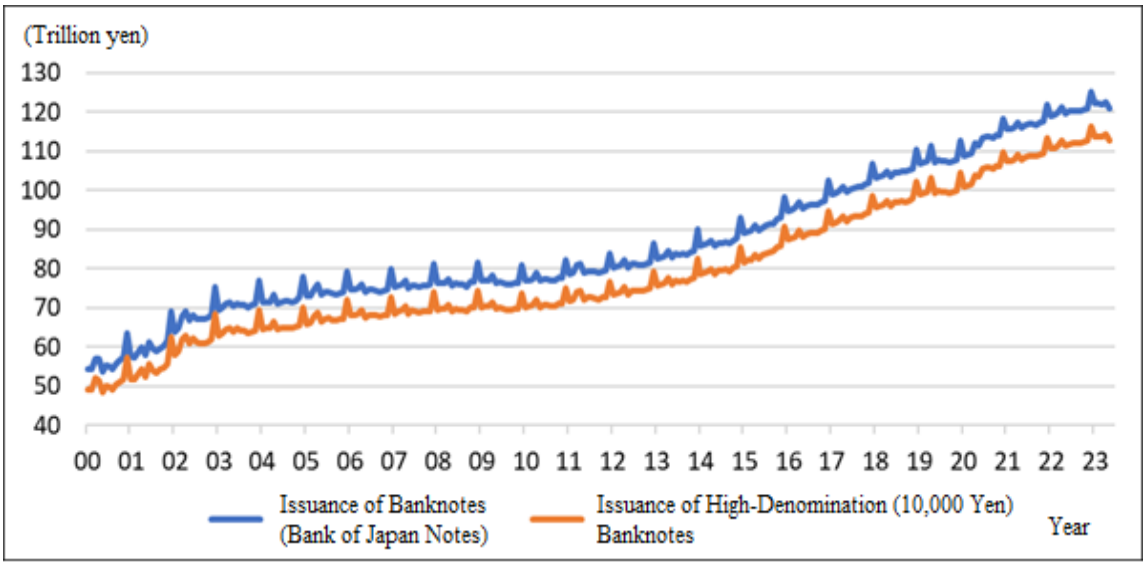
Note: Based on the National Survey of Family Income, Consumption and Wealth (previous National Survey of Family Income and Expenditure) by the Ministry of Internal Affairs and Communications.

Table16: Ratio of Cash Distribution Balance for Different Countries in Nominal GDP



Note: Based on CIS Statistics Explore.

Table 17: Trends in the Issuance of Banknotes (Bank of Japan Notes) and High-Denomination (10,000 Yen) Banknotes



Note: Based on the Currency in Circulation of the Bank of Japan.

(B)Typologies

The main cases where cash transactions were misused for money laundering between 2020 and 2022 are as follows:

- ○ Offenders obtained cash by selling or pawning stolen items in the name of a fictitious or other party at secondhand shops, pawnshops, etc.
- ○ Cash, which was the proceeds of crime from theft, was exchanged for high-denomination banknotes through relatives unaware of the circumstances.
- ○ An offender converted criminal proceeds in cash from robbery into high-denomination banknotes and also deposited them into a bank account under his/her relative's name.
- ○ An offender received criminal proceeds from online and telephone fraud, which were transferred to an account under fictious or other party's name, and withdrew them in cash at an ATM.

(ii)Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds and Enforcement Order requires specified business operators who operate financial businesses, etc., 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 etc., exceeding the equivalent of 1 million yen (100,000 yen in a case bound for North Korea) to notify 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 to prevent the illicit export of cash and other items abroad.

These measures are considered to contribute to reducing risks associated with cash transactions.

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), etc. This is expected to show opaque cash assets, prevent opaque cash circulation, and control ML/TF associated with cash transactions.

Examples of measures that specified business operators implement in order to mitigate risks 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 strict 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.

(iii)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) Characteristics

With a nominal GDP of approximately 557.2 trillion yen, an overall export value of approximately 98.175 trillion yen and an overall import value of approximately 118.141 trillion yen, Japan has been occupying an important position in global economy. Japan also has a highly advanced financial market and conducts a large number of transactions as one of the leading international financial markets around the world, an enormous number of transactions are conducted. As indicated above, although Japan routinely conducts transactions with other countries (including regions, same hereinafter), cross-border transactions have the nature that making it more difficult to track transfer of funds than domestic transaction. This attribute to the fact that domestic legal and transaction systems vary from country to country, and AML/CFT measures such as monitoring and supervision implemented in one country may not be applied in other nations. There are certain countries and regions that allow officers and shareholders of a legal person to be registered under the names of third parties. It is recognized that insubstantial legal persons established in such countries and regions are being misused to conceal criminal proceeds.

Also, passing through such multiple high-anonymity corporate accounts will increase risk of the final transfer destination become unclear.

Furthermore, 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.

Particularly in foreign exchange transactions, money often passes through a series of remotely located intermediary banks, according to correspondent contracts[*1] between banks under which payment services are provided. This may significantly hinder the tracing of criminal proceeds. Because a correspondent's financial institution may not have a direct relationship with the remittance originator etc., there is a risk that money laundering could occur unless the correspondent's institution (the other party to a correspondent contract) develops internal control systems for AML/CFT. Furthermore, if a correspondent's financial institution is a fictitious bank that does not actually do business (what is called a "shell bank"), or if a correspondent's financial institution allows shell banks to use accounts provided by the correspondent, there is a high risk that foreign-exchange transactions could be used for ML/TF.

In recent years, cross-border money laundering offences by international criminal organizations have been recognized in which proceeds from fraud committed abroad are transferred to financial institutions in Japan. Several reasons are believed to be behind these offences. For example, our financial system is highly trusted by the international community, and the detection of crime can be delayed because of the time difference between Japan and the countries in which offences occur.

In addition to the aforementioned bank-to-bank exchange transactions based on correspondent banking relationships, cash courier transactions and transfers of crypto-assets in international dealings can also be potential methods for ML/TF.

Furthermore, international interest in AML/CFT measures is rapidly increasing, and there have been many cases where authorities have imposed heavy fines due to inadequate measures. In light of these circumstances, financial institutions engaging in foreign exchange transactions are required to take actions not only in Japan, while duly considering overseas trends, such as supervisory oversight by domestic and foreign authorities.

---

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

(B) Typologies

Analysis of cases in which cross-border transactions were misused revealed that not only offenders committing crimes in Japan, but also international crime organizations and foreigners, are involved in such cases. Money laundering is an internationally recognized crime.

The modus operandi used in the above cases include:

○ To misuse financial institutions, etc., in and outside Japan (cross-border remittances, etc.);

○ To disguise money laundering as legal trading (export or import of goods, etc.);

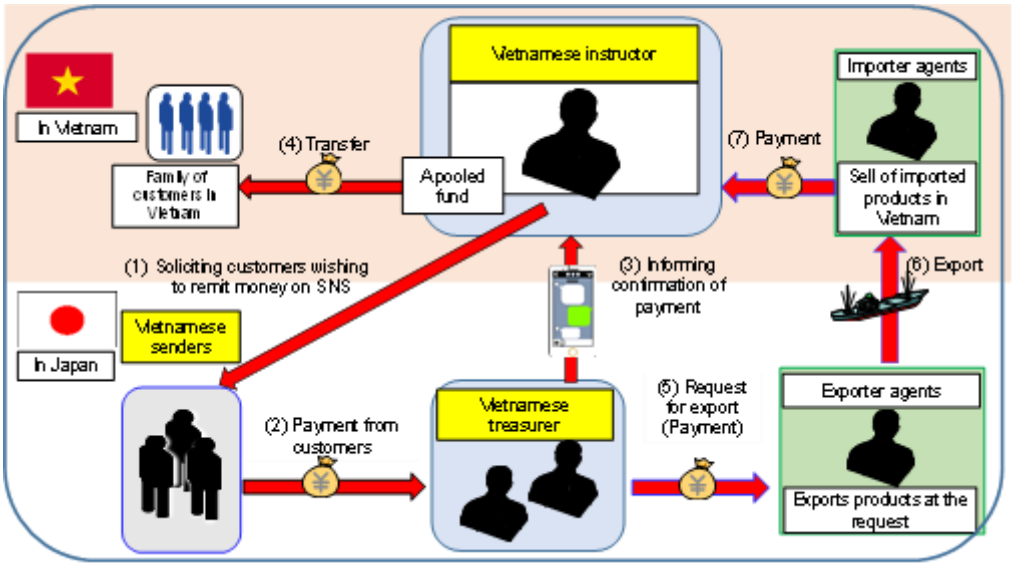
○ To provide domestic and cross-border remittance and payment services without actually moving funds;

○ To use cash couriers, and

○ To misuse the transfer of crypto assets.

There are examples of criminal activities carried out through these methods, such as so-called underground banks (see Table 18). In the case of underground bank incidents, there are instances where multiple deposits in the names of foreign individuals are allowed into accounts managed by vault keepers, whether they belong to the actual account holder or are in fictitious or other parties' names.

Table 18: Cases of Underground Banking Offences by Vietnamese



Specific characteristics of modus operandi used in money laundering cases, in which offenders try to hide the true source of funds or facts about funds by disguising criminal proceeds from fraud committed overseas 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 money laundering cases or underground banking cases disguised as legal trading, the following characteristics were found:

○ To export goods with export permits obtained by preparing false documents and

○ 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.

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

Regarding money laundering crimes that have exploited transactions with foreign entities between 2020 and

2022, the following incidents have been observed:

- ○ An offender remitted money stolen by fraud (such as business email fraud (BEC)) in America, Europe, etc., to an account opened at a bank in Japan. The Japanese account holder presented a forged invoice, etc., at the bank counter to withdraw the money by pretending to receive money remitted in a legal transaction.
- ○ An offender posted illegal videos on a video-sharing site in another country and received criminal proceeds by disguising the cross-border remittances of payments for the videos as remittances for legal transactions.
- ○ An offender illegally made victims transfer money to an account in a foreign country by disguising the transfer as a legal funds transfer by a company to purchase crypto assets with the stolen money.
- ○ An offender met victims through social media, etc., and made them transfer money stolen from them to a bank account in fictious or other party's name, and then transferred the money to a bank account opened by a criminal group in another country by disguising the transfer as a legal cross-border remittance.
- ○ When transferring fraudulent proceeds abroad, false reasons for the transfer were stated in the transfer reason section of related documents, and false invoices 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.
- ○ Proceeds obtained from child pornography crimes were deposited into accounts in the perpetrator's name within the country, originating from foreign banks. False reasons for the deposits were declared to bank officials, disguising them as legitimate business income.
- ○ To bring assets owned abroad into the country, false reasons for use were declared to relatives to fraudulently open domestic bank accounts, and legitimate transactions were pretended as overseas assets were transferred to the same accounts.

(C) Trends of STRs

The number of notifications of STRs related to cross-border remittances between 2020 and 2022 was 133,767 , with transactions involving China as the destination or origin of remittances accounting for 27.6%. Additionally, in 2022, notifications of transactions involving Vietnam as the destination or origin of remittances have significantly increased (refer to Table 19).

Table 19: Annual Number of Notifications of STRs Related to Cross-border Remittances

Destination (origin) Country or Jurisdiction	2020	2021	2022	Total	Percentage (%)
China	13,918	11,685	11,286	36,889	27.6
Hong Kong	5,525	4,848	3,900	14,273	10.7
USA	4,553	4,150	3,866	12,569	9.4
Vietnam	946	1,772	5,714	8,432	6.3
South Korea	2,429	3,159	1,749	7,337	5.5
Taiwan	2,208	2,124	1,975	6,307	4.7
United Kingdom	1,849	1,684	1,633	5,166	3.9
Philippines	1,208	1,755	2,146	5,109	3.8
Singapore	1,500	1,353	1,718	4,571	3.4
Russia	927	901	917	2,745	2.1
Thailand	985	780	716	2,481	1.9
Australia	591	548	696	1,835	1.4
United Arab Emirates	549	534	709	1,792	1.3
Indonesia	512	485	599	1,596	1.2
Cambodia	451	400	637	1,488	1.1
Malaysia	527	494	388	1,409	1.1
Canada	434	495	444	1,373	1.0
Switzerland	390	372	293	1,055	0.8
Germany	383	295	233	911	0.7
Turkey	284	239	256	779	0.6
Others	5,659	5,278	4,713	15,650	11.7
Total	45,828	43,351	44,588	133,767	-

(ii) Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify the purpose and intended nature of the business relationship when they conduct specified transactions[*1]. In addition, the Act provides that certain specified business operators (financial institutions, etc. 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, specified business operators must provide customer identification data of the originator to the institution; and, they must preserve customer identification data provided by a foreign-exchange transaction operator whose country has similar legislation.

In December 2022 due to the revision of the Act on Prevention of Transfer of Criminal Proceeds, when specified business operators conduct foreign exchange transactions, in addition to information on customers, they are

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

newly required to provide information on payment counterparties to other specified business operators or exchange business operators located abroad.

In the Supervision Guidelines 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 specified the points to consider when supervising the execution of correspondent contracts.

Additionally, the Financial Services Agency has also 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, etc.

To reduce the degree of risk related to cash couriers, the FEFTA requires those who export or import the means of payment such as cash or checks etc., or securities exceeding the equivalent of 1 million yen (100,000 yen in a case bound for North Korea), or over 1 kg of precious metals[*1] to notify the Minister of Finance in writing and the Customs Act also requires that export or import declarations of goods mentioned above to the Director-General of Customs must be in writing. Customs authorities work closely with relevant agencies to enhance the collection, analysis, and utilization of information and engage in border control efforts to prevent the illicit export of cash and other items abroad.

The Ministry of Finance specified the details of inspection, etc. related to the development of systems, etc. 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, etc. These measures are considered to contribute to reducing the risk associated with transactions with foreign entities.

Examples of specified business operators' measures to reduce the degree of 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 submit STRs by focusing on the discrepancy between the purpose of remittances from foreign countries and the recipients' usage of funds.
- ○ 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 transactions with foreign countries, it is not easy to trace transferred funds compared to domestic transactions because of the difference in legal systems and transaction systems.

In fact, in some cases, money laundering 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 international organized crime in Japan, criminal organizations composed of foreigners visiting Japan commit crimes under the direction of criminal organizations existing in their country of origin. Their networks and criminal acts are not in only one country. Roles are divided across national borders. As a result, crime is becoming

---

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

more sophisticated and latent. There is also a risk that criminal proceeds obtained by criminal organizations consisting of foreigners in Japan will be transferred back overseas.

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 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.

2. Countries/Regions

We identified, analyzed, and assessed countries/regions that may influence transaction risks 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) and the like.

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 members to take AML/CFT measures in consideration of risks arising from the deficiencies. Those countries/regions identified as High-Risk Jurisdictions subject to a Call for Action[*1] have been published as the "blacklist".

A 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 and other jurisdictions to apply countermeasures 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 upon all member countries and other jurisdictions to apply countermeasures against Iran, however, in June 2016, the FATF evaluated the measures taken by Iran and suspended 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 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 Recommendations (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. The FATF requests all member countries, as well as other countries and regions, to completely terminate the temporary suspension of the countermeasures against Iran and apply the countermeasures from February 2020 in light of Iran's failure to develop internal collateral laws for executing the United Nations Convention against Transnational Organized Crime and international agreements to prevent the provision of funds for terrorism according to the FATF standards.

(iii) Myanmar

In its October 2022 statement, the FATF, considering that Myanmar has not made significant progress in addressing serious deficiencies in AML/CFT measures, has called upon all member countries and other jurisdictions to apply enhanced CDD measures commensurate with the risks emanating from Myanmar. Based on this statement, transactions with Myanmar are recognized as having a high risk of ML/TF.

2. Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds and Enforcement Order stipulates that Iran and North Korea are jurisdictions deemed to have inadequate AML/CFT systems (hereinafter referred to as "specified jurisdictions") and

---

* High-Risk Jurisdictions subject to a Call for Action

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), etc. 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 Jurisdictions under Increased Monitoring for improving the AML/CFT measures. The FATF is calling on those countries/regions[*2] 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. Also, 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.

---

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

* 2 Jurisdictions under Increased Monitoring, as designated within the monitoring process.

[Changes in Countries/Regions for Which the FATF Requested Its Members and Other Jurisdictions to Apply Countermeasures, etc., in the FATF Statements or Designated as under the FATF's Monitoring Process to Improve AML/CFT Measures]

The following list shows when decisions were made and announced over the last three years (2021 to 2023) regarding the designation of countries/regions for which the FATF requested its members and other jurisdictions to apply countermeasures, etc., 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 June 2023, with countries/regions publicly disclosed at the time of the FATF plenary meetings listed in Table 20 and countries/regions that have been disclosed in the past listed in Table 21.

Table 20: Countries/Regions for which the FATF called on its members and other jurisdictions to apply countermeasures

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

Country/Region/ Period	2021			2022			2023	
	Februar	June	October	March	June	October	Februar	June
Iran	●	●	●	●	●	●	●	●
North Korea	●	●	●	●	●	●	●	●
Myanmar						◎	◎	◎

Table 21: 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	2021			2022			2023	
	February	June	October	March	June	October	February	June
Albania	○	○	○	○	○	○	○	○
Barbados	○	○	○	○	○	○	○	○
Burkina Faso	○	○	○	○	○	○	○	○
Cameroon								○
Cayman Islands	○	○	○	○	○	○	○	○
Croatia								○
Democratic						○	○	○
Gibraltar					○	○	○	○
Haiti		○	○	○	○	○	○	○
Jamaica	○	○	○	○	○	○	○	○
Jordan			○	○	○	○	○	○
Mali			○	○	○	○	○	○
Mozambique						○	○	○
Nigeria							○	○
Panama	○	○	○	○	○	○	○	○
Philippines		○	○	○	○	○	○	○
Senegal	○	○	○	○	○	○	○	○
South Africa							○	○
South Sudan		○	○	○	○	○	○	○
Syria	○	○	○	○	○	○	○	○
Tanzania						○	○	○
Turkey			○	○	○	○	○	○
Uganda	○	○	○	○	○	○	○	○
United Arab				○	○	○	○	○
Vietnam								○
Yemen	○	○	○	○	○	○	○	○

Country/Region /Period	2021			2022			2023	
	February	June	October	March	June	October	February	June
Botswana	○	○						
Cambodia	○	○	○	○	○	○		
Ghana	○							
Nicaragua	○	○	○	○	○			
Malta		○	○	○				
Mauritius	○	○						
Morocco	○	○	○	○	○	○		
Pakistan	○	○	○	○	○			
Zimbabwe	○	○	○					

* For the situation in each country, refer to the original text of the statement, "Jurisdictions under Increased Monitoring-June 2023" (https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-june-2023.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 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

We identified, analyzed, and assessed the customer types that affect transaction risks by referring to cleared cases in which Boryokudan gangsters committed money laundering and severe terrorism situations; circumstances that increase the risks of ML/TF listed in the Interpretive Notes to the FATF Recommendations ("non-resident customers" and "ownership structures of companies that appear unusual or excessively complex," etc.); 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]"), and the like.

○ Persons who intend to commit ML/TF:

(1) Boryokudan etc.[*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, etc.)

(1) Boryokudan etc.

In Japan, Boryokudan, etc. not only commit various crimes to gain profit but also conduct fundraising activities by disguising them as or misusing business operations.

Essentially, Boryokudan are typical criminal organizations in Japan. They commit crimes habitually and/or in an organized manner to gain profit.

Boryokudan exist throughout Japan, but their size and activities vary. As of October 1, 2023, 25 groups are listed as designated Boryokudan under the Anti-Boryokudan Act.

At the end of 2022, the total number of Boryokudan gangsters was 22,400[*3] including 11,400 Boryokudan members and 11,000 associates [*4]. The totals of these numbers have been declining continuously since 2005 and are the smallest since 1992 in which the Anti-Boryokudan Act was enforced. We believe that this is because members withdrew from Boryokudan due to the development of activities to exclude Boryokudan and the enforcement of supervision in recent years, resulting in difficulty in conducting fund-raising activities. On the other hand, it seems that one result of recent stronger crackdowns on Boryokudan is that the number of people who do not formally belong to an organization despite strong ties with Boryokudan is increasing, and that activities of those surrounding Boryokudan and their relationship with Boryokudan are diversifying.

Also, in recent years, groups equivalent to Boryokudan in which persons belonging to the groups perpetrate violent illegal behavior, etc. such as collectively and habitually committing violent acts even though they do not have a clear organizational structure as Boryokudan does (hereinafter referred to as "quasi-Boryokudan") engaging themselves in

---

*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 the 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.

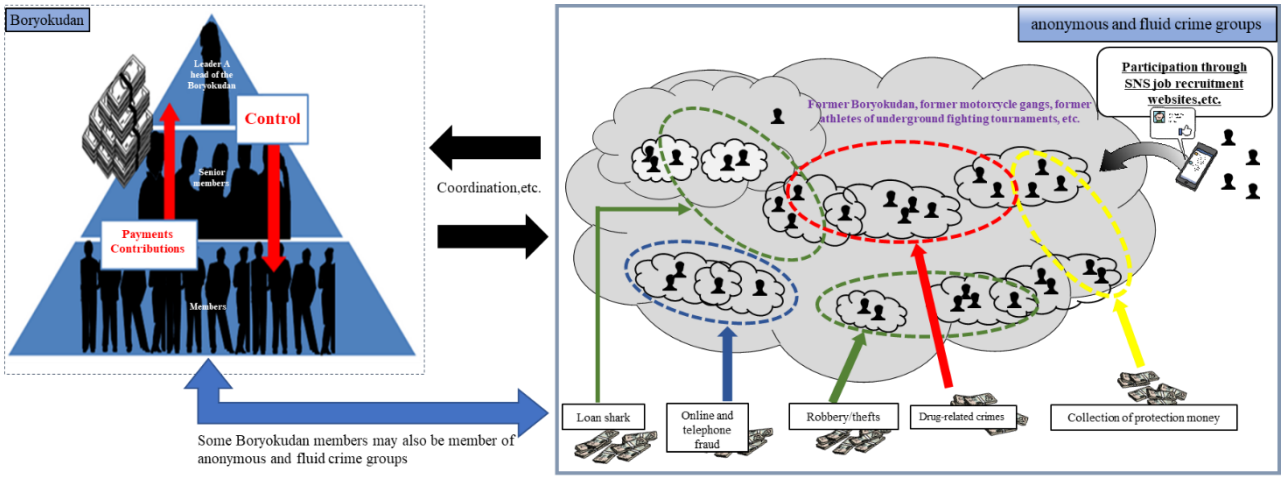
*2 In this NRA-FUR, "Boryoudan etc." refers to Boryoudan (organized crime groups), anonymous and fluid crime groups, Boryoudan-affiliated companies, Sokaiya" racketeers, person(s) engaging in criminal activities under the pretext of social campaigns or political activities, and violent groups/individuals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

*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, etc. by utilizing the power of Boryokudan, or cooperate or are involved in the maintenance or operation of Boryokudan by offering funds or weapons, etc. to Boryokudan or Boryokudan members.

violent, illegal acts habitually. In recent years, there have also been groups beyond those classified as quasi-Boryokudan that use methods such as recruiting perpetrators through social media, job recruitment websites, etc., to carry out online and telephone fraud, etc. widely, posing a threat to public safety. These groups, through loosely connected interactions such as via social media, exhibit fluid relationships characterized by fluctuations in their connections. They leverage highly anonymous communication methods and often divide roles among themselves. Additionally, they accumulate funds through illegal activities like online and telephone fraud and robbery, using these funds to anonymize further and conceal their activities. Some of these groups expand into additional illicit activities or business ventures, such as the entertainment industry, using the acquired funds as a base. In light of this situation, the police categorize such groups, including quasi-Boryokudan, as "anonymous and fluid crime groups" and are actively working towards understanding their actual activities. Furthermore, it has been observed that some anonymous and fluid crime groups maintain relationships with Boryokudan by contributing a portion of their funds, and there have been instances where Boryokudan members conspire with anonymous and fluid crime groups to commit crimes.

Table 22: Structure of Boryokudan and Anonymous and Fluid Crime Groups



(i) Factors that Increase Risks

(A) Characteristics

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 general economic transactions by using Boryokudan-affiliated companies which are substantially involved in their management or conspiring with persons who cooperate with or assist in the money-making activities*[1], etc. 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 money laundering 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, etc. Criminal proceeds may also be

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

used to interfere with legal businesses.

Furthermore, anonymous and fluid crime groups are actively engaging in illegal fund-generating activities, such as online and telephone fraud, etc. while coexisting and thriving alongside Boryokudan and others. They use the funds obtained through these activities as capital to expand into various industries, including the adult entertainment industry, the entertainment sector (such as adult videos), and scouting. They also engage in money laundering and serve as a source of talent for online and telephone fraud.

In light of the fact that the number of cleared cases of money laundering involving Boryokudan gangsters has been stable even though the total number of Boryokudan gangsters is decreasing, it is considered that money laundering is still necessary for Boryokudan gangsters to obtain funds. Boryokudan and anonymous and fluid crime groups collude while evading restrictions under the Anti-Boryokudan Act and the Organized Crime Exclusion Ordinances, etc. to skillfully obtain funds. Therefore, to grasp the actual state of these fund-raising activities, it is necessary for the public and private sectors to cooperate in combating such activities.

(B) Typologies

From 2020 through 2022, there were a total of 1,958 cleared cases of money laundering, of which 186 cases, or 9.5% of the total, had clear involvement of Boryokudan gangsters.

During this period, some of the main instances where Boryokudan gangsters were involved in money laundering included the following cases:

- ○ Boryokudan members received criminal proceeds from illegal gambling, prostitution or unlicensed adult-entertainment business, etc. in cash by calling the proceeds so-called “protection money,” knowing that they were criminal proceeds.
- ○ Boryokudan members withdrew cash deposited into accounts under the name of fictitious or other parties through online and telephone fraud. Then, they transferred it to their accounts, which were then further transferred to different accounts managed by others.
- ○ Former Boryokudan members 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 steal money from financial institutions by calling it a loan for fictitious business and used an account in the name of his acquaintance or relative.
- ○ A Boryokudan member used a fake name to sell stolen goods.

The following facts have been revealed from the money laundering 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 money laundering using methods that make tracing of criminal proceeds difficult.

(ii) Trends of STRs

The number of STRs submitted during the period from 2020 to 2022 was 1,545,669, including 182,314 STRs submitted for reasons related to Boryokudan, accounting for 11.8% 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) have been formulated to help companies to cut any relationships with Boryokudan etc.

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, etc., are introducing clauses to exclude Boryokudan, etc. 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, etc. Furthermore, if a customer has turned out to be a member of Boryokudan, etc., financial institutions, etc. 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 overseas databases at the start of transactions and even after the start of transactions. If a customer turns out to be a member of Boryokudan etc., 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 about Boryokudan information through the Deposit Insurance Corporation of Japan for applicants of new personal loan transactions to banks.

(iv) Assessment of Risks

Other than committing various crimes to gain profit, Boryokudan etc. conduct fundraising activities by disguising them as or misusing business operations. As money laundering makes the source of funds from criminal activities or fundraising activities unclear, money laundering is indispensable for Boryokudan etc. Since Boryokudan etc. engage in money laundering, transactions with Boryokudan etc. are considered to present high risk. Also, these days, Boryokudan are actively engaging in activities to obtain funds in society while concealing the state of their organizations. 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 (Such as Islamic Extremists)

Current international terrorism issues remain severe, with terrorist attacks occurring in various countries, including Europe and the U.S. Additionally, there is a concern that foreign fighters who participated in battles in Iraq and Syria may commit acts of terrorism after returning to their home countries or moving to third countries. As the threat of terrorism has spread across borders, it is essential that countries cooperate with each other in implementing countermeasures against terrorist financing. The matters which should be paid attention to in terms of terrorist financing have increased and become more complicated. Thus, in this NRA-FUR, identified ISIL, AQ and other Islamic extremists, foreign fighters, and individuals who have become extremists (hereinafter collectively called "Islamic Extremists") as customers who may become factors that affect risk, referring to the FATF Recommendations, its Interpretive Notes, the FATF's reports, and measures under the Act on Prevention of Transfer of Criminal Proceeds, taking the following into account:

○ Threats (terrorist groups such as ISIL, AQ, and other Islamic extremists and their financiers)

○ Vulnerabilities (legal and illegal sources and methods of terrorist financing)

and comprehensively considering these factors including their impacts on Japan.

(i) Factors that Increase Risks

(A) International Terrorism Situation

ISIL, which declared the establishment of a caliphate in 2014, briefly expanded its influence in Iraq and Syria. However, it has lost control over both countries due to attacks by Iraqi and Syrian forces with the support of various foreign nations.

In 2022, the second and third leaders were successively killed by foreign operations, including U.S., and in 2023, the fourth leader was also killed, and a fifth leader was announced to assume leadership.

ISIL has consistently carried out 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. ISIL has called for attacks using knives, vehicles, and other means when individuals cannot obtain explosives or firearms for executing acts of terrorism. In 2022, there were still terrorist incidents committed by individuals believed to be influenced by the extremist ideology of ISIL and other groups.

Furthermore, in the Sahel region of Africa and other areas, Islamist extremist groups, which ISIL claims as their "provinces," have been actively carrying out terrorist attacks on local military installations and other targets. There is also a concern about the risk posed by foreign fighters from Iraq and Syria traveling to their home countries or third countries to carry out acts of terrorism. Additionally, the possibility of further radicalization within detention facilities or refugee camps is being raised.

Additionally, AQ and its affiliated organizations have repeatedly espoused anti-American and anti-Israeli ideologies, calling for terrorist actions in Western countries through their online publications etc. In July 2022, the leader of AQ, Ayman al-Zawahiri, was killed because of U.S. operations. However, AQ-affiliated groups operating in the Middle East and Africa continue to carry out attacks targeting local government entities etc. The impact of Zawahiri's death on these affiliated organizations is believed to be limited. In Afghanistan, which was taken over by the Taliban in August 2021, the unstable situation is still ongoing, as the ISIL-K[*1], which has expanded its influence, carried out a suicide bombing in front of the Russian Embassy in Afghanistan in September 2022. The Taliban has been closely linked to AQ, and there are concerns that Islamic extremist organizations' activities will intensify in the country.

In Japan, there are people claiming to be in touch with persons affiliated with ISIL and those who express their

---

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

support for ISIL on the Internet. There was also a case where internationally wanted fugitive on ICPO's list illegally entered Japan in the past. These facts indicate 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, etc. could commit terrorism in Japan.

Table 23: Number of International Terrorism Cases

Item/year	2019	2020	2021
Number of cases	8,872	10,167	8,354
Number of deaths and injuries	26,273	29,366	23,692

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

Table 24: Major Terrorism Cases in 2022

Date	Case
March 27	Gun attack terrorist incident in Hadera, Israel.
June 25	Gun attack terrorist incident in Oslo, Norway.
September 5	Suicide bombing terrorist incident in Kabul, Afghanistan.
October 29	Bombing terrorist incident in Mogadishu, Somalia.
November 10	Knife attack terrorist incident in Brussels, Belgium.
November 13	Bombing terrorist incident in Istanbul, Turkey.

Note: Excerpted from the National Police Agency's Review and Prospects of Public Safety in 2022.

(B) Characteristics

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. No terrorist activity by terrorists designated by the United Nations Security Council has been confirmed in Japan.

Yet it is recognized that criminals who are internationally wanted through the International Criminal Police Organization for murder and attempted bombing, other crimes, have illegally entered and left Japan repeatedly in the past. This indicates that the network of Islamic extremist groups loosely connected through radical beliefs is extending to Japan. Additionally, there are people in Japan who support ISIL or sympathize with the group's propaganda. The Japanese Government authorities have ascertained that there were individuals who had attempted to travel from Japan to Syria to join ISIL as fighters.

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, and monetary assistance provided to foreign fighters by their families, etc. 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 money laundering, 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 going there directly.

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 money laundering.

○ Customer attributes

Customer identification data, including names, aliases, and birthdates, 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.

By taking into account the following pointed out 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 methods

- 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 officer 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) Overseas cases

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

---

*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.

- 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 overseas 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 Crypto-asset Usage for Terrorist Financing (United States)

  In August 2015, an American, Person A, was sentenced to 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. They 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.

- 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 submitted STRs regarding transactions suspected to be related to terrorism financing. Looking at the reasons for submitting these STRs, it was not only because 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 but because terrorist financing is suspected based on the customer attributes and transaction types. Specified business operators are considered to be actively submitting STRs related to terrorism financing. 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

Legislative measures to mitigate risks of the abovementioned terrorist financing include the following.

○ 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 crimes of money laundering. Terrorist funds may be regarded as criminal proceeds under the Act. Therefore, 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.

In addition, each time the list of groups subject to asset freezing and other countermeasures, adopted as United Nations Security Council resolutions (No. 1267 and its succeeding resolutions and No. 1373) 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

The Act on Punishment of Terrorist Financing 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.

The Act on Punishment of Terrorist Financing defines certain offences, including murder or aircraft hijacking, performed for the purpose of threatening the general public or national, local, or foreign governments as “acts of public intimidation” (Article 1). The Act includes provisions to punish certain acts, such as when a person who intends to engage in an act of public intimidation 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, or when someone provides Funds, etc. for collaborators who intend to provide Funds, etc. for a person who intends to provide Funds, etc. for a person who intends to engage in an act of public intimidation (Articles 2 to 5), etc.

With the enactment of the FATF Recommendations Compliance Act on December 29, 2022, the Act on Punishment of Organized Crimes has been amended to strengthen international efforts against terrorist financing further. A new category, i.e., specified criminal activities, has been established to extend the scope of criminal acts subject to charges related to the provision of funds. Additionally, to enhance the deterrence of financing terrorism under international collaboration, the statutory penalties under this Act have been increased.

○ FEFTA

With respect to international transactions, in response to the United Nations Security Council resolutions (No. 1267 and its succeeding resolutions and No. 1373) 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. Specifically, as of June 9, 2023, 398 individuals and 119 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, etc., 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), measures such as freezing assets have been taken against designated individuals and entities under the International Terrorist Asset-Freezing Act. Specifically, as of June 9, 2023, the names of 398 individuals and 119 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

The Strategy to Make Japan "the Safest Country in the World," initially formulated in December 2013 under the leadership of the Prime Minister in the Ministerial Meeting on Crime Control, was completely revised. In December 2022, 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 the promotion of anti-money laundering, counter-terrorist financing, and proliferation financing, in line with the recommendations of the FATF.

Relevant ministries and agencies have been working on AML/CFT measures based on these decisions made by the government. In Japan, even those who have not been designated by the United Nations Security Council Sanctions Committee are subject to asset freezes based on United Nations Security Council Resolution 1373 and Cabinet approval[*1]. In November 2019, asset freezing measures were implemented against 5 groups (New People's Army, Al-Shabaab, ISIL in Sinai, Islamic State in Iraq and the Levant in the Middle East and Asia, and Maute Group). In March 2020, similar measures were taken against 3 groups (Indian Mujahideen, Al-Qaeda in the Indian Subcontinent, and Neo-JMB).

While the essential to counter-terrorist measures is to prevent terrorism, the Police have been promoting anti-terrorist measures from the standpoints of both prevention and response to emergencies based on the recognition that if a terrorist attack does occur, it is necessary to minimize damage as well as to suppress and clear the case by arresting the criminal(s) involved.

Specifically, the following measures are promoted:

- ○ Information collection and analysis and thorough investigation
- ○ Enhanced border security in collaboration with related agencies such as the Immigration Services Agency of Japan and Customs
- ○ Promotion of anti-terrorist cooperation between government and private entities
- ○ Protection of critical public facilities

In addition, in December 2022, the National Police Agency and the Financial Services Agency conducted a briefing session for financial institutions and related organizations on countermeasures against terrorist financing. This session aimed to enhance 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). There have been no terrorist acts carried out in Japan by the terrorists designated by the United Nations Security Council so far.

---

*1 The Measures on terrorist asset-freezing on November 12, 2019, and March 31, 2020.

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 overseas 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 people from Islamic countries 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 can prevent their monitoring from being misused.

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)

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

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. The FATF also calls its member countries to prevent nonprofit organizations from being misused by terrorists, etc. Of course, not all nonprofit organizations are at high risk. Since the risk level varies depending on the nature, scope, etc. of activities, the response must depend on the threat and vulnerability of individual organizations. In the FATF recommendations and its interpretive interpretation notes, 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 international examples, 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, etc. may procure funds by abusing lawful companies or nonprofit organizations, etc. and transfer funds through lawful companies or nonprofit organizations, etc., by taking advantage of new financial technology such as crypto assets.

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) Features

A specified nonprofit corporation (hereafter referred to as an “CESNAs”) is an entity primarily focused on conducting specified nonprofit activities as defined in the Act on Promotion of Specified Nonprofit Activities (Act 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 an 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 July 2023, there are 50,183 CESNAs .

The vulnerabilities of CESNAs to exploitation for terrorist financing include:

- ○ Operating in or near regions where terrorist acts occur.

Some NPO corporations 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 overseas partners and the utilization of volunteers.

When CESNAs expand their activities abroad, they frequently collaborate with local partners, and many volunteers participate in their operations. Collaboration with overseas partners and the utilization of volunteers such as this can

*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 “National Strategy and Policy for AML/CFT/CPF (May 19, 2022)” 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.

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.

(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, 2023, there are 9,712 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 transferring funds abroad or managing cash overseas.

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

The degree of risk of TF can be reduced to some extent if each of these public interest corporations appropriately implements effective measures stipulated in laws and regulations, recognizes risks, and takes action against the risks. On the other hand, only a limited number of public interest corporations recognize the risk of abuse of nonprofit organizations for TF, etc., or review the risk in their business to take action against such risk. Each public interest corporation needs to implement measures under laws and regulations, recognize the risk of TF, and take appropriate measures against the risk faced by each public interest corporation in order to avoid being involved in TF.

Therefore, the Cabinet Office released “Countermeasures Against Terrorist Financing by Public Benefit Corporations” in June 2022, providing specific methods for risk reduction measures to public benefit corporations, along with repeated dissemination of this information.

(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 April 1, 2022, there are 21,053 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 overseas activities 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 implementing overseas activities for social welfare corporations, 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 overseas activities. Furthermore, in the annual status report submitted, specific provisions mandate the clear disclosure of overseas activities, 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 terrorist financing 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, 2023, there are 58,005 medical corporations. As of July 1, 2023, 9 medical corporations are engaged in overseas activities. The overseas activities of medical corporations 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 overseas activities 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 overseas, 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, 2022, there are 7,794 school corporations.

Furthermore, school corporations are established with the purpose of operating private schools and limiting their overseas activities. To analyze the factors and perspectives on the misuse of terrorist financing by school corporations engaged in overseas activities, 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 overseas operations as of 2022.

(ii) Measures to Mitigate Risks

Regarding school corporations' activities, including overseas ventures, 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, 2021, there were 179,952 religious corporations in existence, with approximately 99% of them, or 178,774, falling under the jurisdiction of prefectural governors in a single prefecture. Moreover, around 70% 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 the end of 2022, 3,329 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 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

* 1 Survey report on activities conducted by religious corporations (as of September 2010).

submit the required documents, 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 the required documents are categorized as inactive religious corporations.

Furthermore, we have entrusted the promotion of measures against inactive religious corporations and, along with accumulating examples of such measures, we address the risk of inactive religious corporations being exploited by criminal organizations during prefectural training sessions for religious corporation officials, providing cautionary information to mitigate these risks.

(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 of less than 10 million yen, and the largest organization 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 NPOs 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 terrorist financing is high in the following cases, and considering Japan's position and role as an international financial market, we also need 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 overseas. 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.

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, etc., 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, etc. 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, etc., 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, etc.) 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, etc., 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, etc.) 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 consulates in Japan as a gift for issuing the documents needed to apply for statuses of residence or submitting notifications of marriage.

(ii) Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds, Enforcement Order and Ordinance requires specified

business operators to conduct enhanced CDD, including verifying customer identification data, etc., 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, etc.;
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.

(iii) Assessment of Risks

Foreign PEPs have positions and influence that can be misused for ML/TF. Grasp of their identification data, etc., 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, etc.)

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, etc., who provide services for corporations, etc., 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) Characteristics

Legal persons can be independent owners of property. A natural person can change their ownership of property without the cooperation of another natural person by transferring the ownership to a legal person. Furthermore, legal persons have, in general, complex right/control structures related to properties.

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. Therefore, if a property is transferred to a legal person, it enters the complex rights/control structure of a legal person, meaning it can be easy to conceal a natural person who substantially controls the property because the ownership of the property is unclear. Furthermore, it is possible to transfer large amounts of property frequently in the name of corporate business by controlling a legal person.

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 (see Table 25) by registering under the Commercial Registration Act (Act No. 125 of 1963). Looking at the number of registered establishments by type of legal person in recent years, the number of registrations of limited liability companies has increased (see Table 26). 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*[2]. In this way, the procedures for establishment, etc., differ depending on the form of legal person. In general, the procedures for establishing a holding company are less complicated, and the costs necessary for doing so are less in terms of costs necessary upon establishment, new capital investment, capital contribution in kind, and terms of office of executive officers, etc. (see Table 27).

---

*1 Concealment of Beneficial Ownership (July 2018)

*2 A "holding company" collectively refers to a general partnership, a limited partnership, and a limited liability company, which are the companies set forth in the Companies Act (Act No.86 of 2005).

Table 25: Number of Corporations by Major Corporate Type in Japan

Category \ Year	2019	2020	2021
Stock company	2,559,561	2,583,472	2,612,677
General partnership companies	3,343	3,352	3,325
Limited partnership companies	13,540	12,969	12,482
Limited liability companies	113,196	134,142	160,132
Others	68,780	70,436	75,770
Total	2,758,420	2,804,371	2,864,386

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.

Table 26: Number of Registered Establishments by Each Major Corporate Type

Category \ Year	2020	2021	2022
Stock company	85,688	95,222	92,371
General partnership companies	34	16	20
Limited partnership companies	41	33	30
Limited liability companies	33,236	37,072	37,127
Total	118,999	132,343	129,548

Note: The statistics of the Ministry of Justice.

Table 27: Establishment Procedures and Requirements for Each Major Form of Legal Person, etc.

	Stock Companies	Holding 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	60,000 yen	Amount equal to 7/1,000. 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	40,000 yen		
Amount of investment and initial capital	Needs to be included in initial capital, amount not exceeding 1/2 of which can be recorded as capital reserves.	The entire amount can be recorded as the capital reserve.		
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.		

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. In addition, some such countries/regions have adopted the nominee system, under which legal persons' executives and shareholders can be registered in third-party names for privacy protection. There is a risk that these characteristics are used to establish shell companies in countries/regions serving as offshore financial centers and that the shell companies are misused to conceal criminal proceeds.

It is important to ensure that the legal persons are transparent and that their funds are traceable by revealing their beneficial owners. This is to prevent legal persons from being misused for ML/TF. In this regard, in Japan, there are business operators who provide legal persons, etc., with an address, facilities, and means of communication (rental offices and virtual offices) for the sake of business/management, 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. By misusing these services, it becomes possible for a legal person 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, business scale, etc., including corporate registration.

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).

(B) Typologies

The following cases are common examples of misusing unclarified legal persons, etc., for money laundering from 2020 through 2022:

○An offender established a shell company, sold embezzled goods by disguising the sale as a legal transaction, and made buyers deposit payments into an account in the name of the shell company.

○An offender made their accomplice establish a shell company to receive payments for electronic gift cards obtained through online and telephone fraud at an account in the name of the shell company.

○An offender established a shell company using the names of their acquaintances, then opened a bank account under the company's name and deposited proceeds of crime obtained from embezzlement within their professional duties.

○An offender used an account in the name of a company owned by their accomplice, who provided services for a company in financial difficulties to have victims transfer money stolen by fraud, etc., in a foreign country to the account and withdrew stolen money by disguising the money transfers as remittances for legal dealings.

○In another instance, criminal proceeds acquired through fraud and other illicit means were transferred overseas into a bank account opened under the name of a shell company, using a fabricated purpose for the remittance.

Looking at the cleared cases of money laundering offences, etc., in which legal persons were abused in Japan, it is found that those who intend to engage in ML, etc., abuse the following characteristics of legal persons:

○ Take advantage of trust in transactions

○ Frequently transfer large amounts of assets

○ Commingle criminal proceeds, etc., with legal business income, which enables them to obscure sources of illegal income

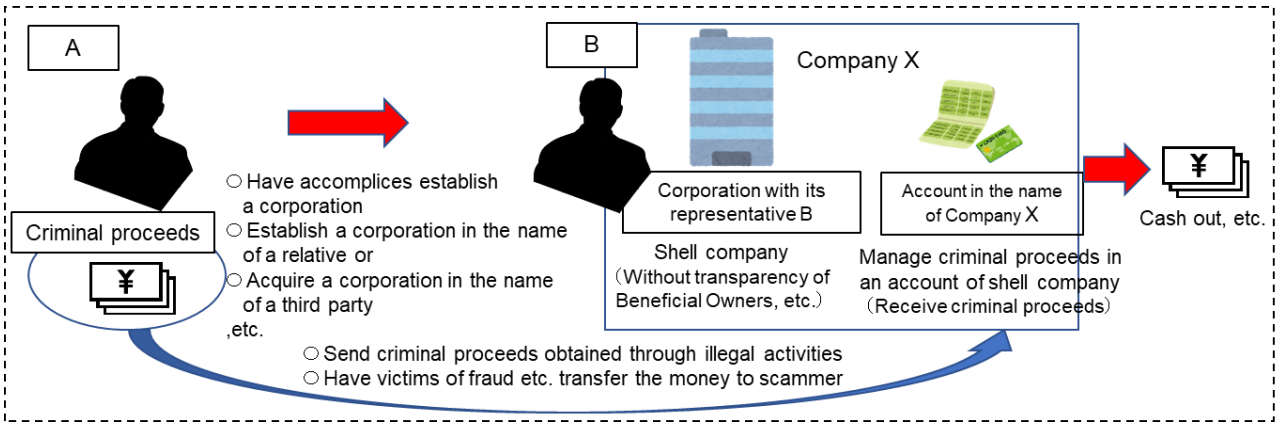
Among modus operandi of misusing legal persons, it is difficult to track criminal proceeds in case of misuse of legal persons whose actual status of business activities or beneficial owners is unclear. Specifically, the following are example cases:

○ A dummy legal person is established for the purpose of misusing it to conceal criminal proceeds.

○ A person who intends to conceal criminal proceeds illegally obtains a legal person owned by a third party.

We have recognized situations where legal persons are controlled through the above modus operandi to misuse bank accounts in the name of such legal persons as destinations to conceal criminal proceeds.

Table 28: The Image of Money Laundering Misusing Corporations without Transparency of Beneficial Owner, etc.



Of the money laundering offences apprehended from 2020 to 2022, 36 involved the exploitation of shell or opaque corporations. Of these, 6 offences exploiting shell or opaque corporations occurred in 2022, involving a total of 11 corporations. Among the exploited corporations, categorized by their legal structure, there were 9 stock companies (including special limited liability company), 1 limited liability company, and 1 other type of corporation.

By analyzing the abused companies in the register, it was revealed that the abused companies include the following types of companies:

- ○ Companies established with a very small amount of initial capital (tens of thousands to hundreds of thousands of yen);
- ○ Companies that frequently change locations or officers in the register; and
- ○ Companies with suspicious operations, such as those that have various purposes of business not closely related to each other in the register.

When analyzing the period between the establishment of companies and abuse of them, it was found that many of the limited liability companies in question were abused within a shorter period of time after establishment than stock companies. Some limited liability companies were abused within a few months after establishment. Looking at the predicate offences in the cases of abuse of legal persons, fraud, including fraud in foreign countries, accounts for the largest percentage. Such predicate offences also include violation of the Investment Act or the Money Lending Business Act, distribution of obscene goods and, embezzlement in pursuit of social activities, etc. It was also found that shell companies or opaque companies are abused for offences committed by criminal organizations continuously and repeatedly in order to generate large amounts of proceeds.

(ii) Trends of STRs

The customer attributes, details of business, and forms of transactions, etc., 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 is Boryokudan.
- ○ A representative director of a company, who is a foreigner, is under the status of residence with restrictions on employment.
- ○ The purposes of business in the register are unreasonably diverse and not closely related to each other.
- ○ The submission of documents, including identification documents, was refused, or the business details or transaction purposes were not explained appropriately.
- ○ 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, etc.
- ○ A substantially dormant 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.
- ○ Entities that suddenly engage in high-value transactions use accounts at multiple crypto-assets exchange businesses, including both corporate and individual accounts, across various devices and exhibit behavior indicative of shared login information

(iii) Measures to Mitigate Risks

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.

Law	Provisions
Act on Prevention of Transfer of Criminal Proceeds and Ordinance	Defines a beneficial owner and requires specified business operators to verify the identity of a beneficial owner of a customer, etc., which is a legal person. Requires specified business operators performing services to provide companies, etc., 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, etc.
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, etc.
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.

Furthermore, 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 addition, the Companies Act stipulates the dissolution of companies deemed to be dormant[*1]. This is 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 32,000 cases in fiscal 2020, 30,000 cases in fiscal 2021, and 29,000 cases in fiscal 2022.

(iv) Assessment of Risks

Legal persons can make the rights and controlling interests in their properties complicated. Beneficial owners of legal persons can conceal the fact that they have substantial rights to such properties by making their properties belong to legal persons. Therefore, it is considered that there are risks in engaging in transactions with legal persons.

Looking at the risks in the form of a legal person, existing stock companies are at risk of abuse, considering that they are established through strict procedures, etc., hold a high degree of trust from the general public, and their shares can be easily transferred. On the other hand, newly established holding companies are at a risk of abuse, considering that they are generally established through simple procedures and can be maintained at low cost.

In addition, due to these characteristics of legal persons, it is not easy to trace funds owned by legal persons, particularly those without transparent beneficial owners. There are examples of cases where a bank account, which was opened in the name of a legal person without a transparent beneficial owner, was misused to conceal criminal proceeds derived from fraud and other crimes. Considering this, it is recognized that transactions with legal persons that do not have transparent beneficial owners present a high risk for ML/TF.

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

Section 5. Risk of Products and Services

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

(1) Products and Services Dealt with by Deposit-taking Institution[*2]

(i) Factors that Increase Risks

(A) Characteristics

Deposit-taking institutions such as banks must obtain licenses from the Prime Minister under the Banking Act, etc. As of the end of March 2023, 1,344 institutions have obtained the licenses, etc. They are mainly banks (134 banks, except branches of foreign banks) and cooperative financial institutions (254 Shinkin Banks, 145 Credit Cooperatives, 13 Labour Banks, 620 agricultural cooperatives and fisheries cooperatives, and 42 credit federations of agricultural cooperatives and credit federations of fisheries cooperatives). Among these institutions, banks held a total deposit balance[*3] of 115,276.2 billion yen for a total of 788.67 million accounts as of the end of March 2023.

Acceptance of deposits, etc., loan of funds, discounting of bills, and exchange transactions (domestic and foreign exchange) are inherent business operations[*4] 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, etc.

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 in which some cross-border crime organizations have transferred funds illegally obtained by fraud, etc., in foreign

---

* [1]The products and services handled by each specified business operator are described in this 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 this NRA-FUR into consideration according to the products and services they handle.

* [2]Deposit-taking Institutions mean those listed in Article 2, paragraph 2, items 1–16 and 37 of the Act on Prevention of Transfer of Criminal Proceeds (banks, Shinkin banks, etc.).

* [3]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.

* [4]Business stipulated in the Banking Act, Article 10, paragraph 1, each item.

countries through Japan's financial institutions as part of their money laundering process.

In addition, the majority of transactions, excluding cash deals, which were illicitly used for money laundering in the past three years, were domestic exchange transactions, deposit transactions, and transactions with foreign countries (foreign exchange transactions, etc.) dealt with by deposit-taking institutions.

Due to the above characteristics, the Financial Services Agency evaluates that ML/TF risks for the business type of deposit-taking institutions are higher than those for other business types. 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 "The Anti-Money Laundering/Countering the Financing of Terrorism Guidelines" published by the Financial Services Agency.

On the other hand, through its supervision to date, the Financial Services Agency recognizes that, while there are financial institutions where efforts are lagging, the overall level of preparedness has improved. Among these, the process of reflecting the results of risk assessments based on the products and services provided, transaction types, countries or regions involved in transactions, and customer attributes in documents prepared by specified business operators is becoming widespread among deposit-taking financial institutions. The Financial Services Agency notes that the content of the analysis of ML/TF risks faced by these institutions has also improved in their AML/CFT Risk assessment documents. Moreover, the implementation of ongoing CDD measures that are appropriate to the risk, the use of transaction monitoring systems with risk-based scenarios and thresholds, and the application of transaction filtering systems for matching against lists of sanctioned individuals are being advanced in deposit-taking financial institutions as important risk mitigation measures.

[New Threats and Vulnerabilities, etc. Found by Competent Authorities]

- It was found in the receiving agent's scheme that there are business operators that obtain the receiving agents' rights from a third party to receive deposits at a bank account opened by the third party and send funds in bulk (so-called "bulk remittance*[1]") to other business operators located overseas. There is a risk for banks, as well as for funds transfer service providers, that they cannot verify the identity of persons sending money to customers or persons who eventually receive funds.
- There was a case where a crypto-assets exchange service provider made illegal remittances to a bank account opened at a bank by the crypto-assets exchange service provider (discovered during the monitoring of a major bank's subsidiary). Although offenders and modus operandi have not been identified, there were cases where victims intentionally made funds transfers and cases where a holder's name and number of an account in the name of a crypto-assets exchange service provider were stolen from a victim and funds transfers were made against the victim's will.

(B) Current situation of products/services provided by deposit-taking institutions and misusing cases

(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 convenience is further increasing.

However, because of such characteristics, a deposit/savings account can be used as an effective way to receive and conceal criminal proceeds by those attempting to launder money.

The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct

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

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

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

- ○ Offenders used accounts belonging to foreign nationals who have returned to their home countries without following procedures to close the accounts, etc., or deceased persons to deposit criminal proceeds from fraud and theft, etc.
- ○ 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, etc. to deposit criminal proceeds derived from fraud, theft, loan-shark crime, violation of the Amusement Business Act, drug crimes, and sale of fake brand goods, etc.

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 various ways of acquiring accounts illegally. 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.

Furthermore, there are 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 money laundering offences. In this way, accounts opened under fictitious or other parties are obtained through illegal trading and misused to receive criminal proceeds in online and telephone fraud, loan-shark cases, etc. Criminal proceeds are transferred using such accounts.

Furthermore, the police actively crack down on the following as contributors to the misuse of deposit/savings accounts (see Tables 29 and 30):

- ○ 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 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 29: Number of Cleared Cases of Violating the Act on Prevention of Transfer of Criminal Proceeds

Category \ Year	2020	2021	2022
Transfer of deposit/savings passbook, etc.	2,539	2,446	2,951
Transfer of deposit/savings passbook, etc. (business)	18	27	18
Solicitation and inducement for transfer of deposit/savings passbooks, etc.	32	11	10
Transfer of exchange transaction cards, etc.	35	26	41
Transfer of information for crypto-assets exchange	6	23	46
Others	4	2	0
Total	2,634	2,535	3,066

Table 30: Number of Cleared Cases of Account Fraud etc.

Category \ Year	2020	2021	2022
Account fraud	696	710	733
Transfer of stolen goods	7	1	0
Total	703	711	733

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, those who attempt ML/TF pay attention to the safe and reliable management of funds and the high convenience of deposit transactions that accounts provide, and they attempt to engage in ML/TF by depositing and withdrawing the proceeds of crimes. In online and telephone fraud cases, deposit transactions are actually misused for money laundering. For example, a crime group made victims, including elderly people, transfer money to the deposit/savings accounts of fictious or other parties’ name used by the crime group to withdraw money or transfer money to other deposit/savings accounts.

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 money laundering:

○ An offender withdrew criminal proceeds that were derived from fraud conducted overseas and

transferred to an account in Japan by disguising them as legitimate business proceeds.

- ○ An offender deposited criminal proceeds derived from theft, fraud, loan-shark crimes, drug crimes, and gambling, etc. into accounts opened in fictious or other parties' names.
- ○ An offender deposited a large amount of stolen coins into an account under the name of fictious or other party at an ATM, and then withdrew it in cash at another ATM.
- ○ An offender deposited cash obtained through theft into the account of a relative 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.

(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, domestic exchange transactions can be used as an efficient way to launder money because these characteristics or abuse of an account in the name of fictious or other party can ensure anonymity.

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, etc. 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 money laundering:

- ○ A Boryokudan member received criminal proceeds from unlicensed adult entertainment business as protection money by transfer to an account in his acquaintance's name.
- ○ 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 fictious or other party.
- ○ An offender instructed customers to transfer payments for stimulants or payments to loan sharks to an account under the name of fictious or other party.
- ○ 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 fictious or other parties.
- ○ An offender received compensation for dispatching foreigners illegally staying in Japan to work by transfer to an account in his/her acquaintance's name.

- ○ An offender received money stolen on online auction sites by transfer to an online bank account that he/she opened in his/her acquaintance's name in advance to conceal criminal proceeds.
- ○ Funds were transferred from a corporate account, managed in the course of business, to an unsuspecting acquaintance's account as fictitious salary payments, and then further transferred from that acquaintance's account to the criminal's account.

(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. Such a characteristic means that safe-deposit boxes can be an effective way to conceal criminal proceeds physically.

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 money laundering:

- ○ 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.
- ○ An offender concealed criminal proceeds by using false names to lease safe deposit boxes at many banks (case in a foreign country).

(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 same characteristics also make bills and checks efficient ways to receive or 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 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 money laundering:

- ○ 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 fictious or other party.
- ○ Bills or checks were misused to smuggle huge amounts of funds to a foreign country (case in a foreign country).
- ○ Bills or checks were misused by drug cartels as a way to separately transfer a huge amount of money (case in a foreign country).

[Electronic Payment Handling Services, etc.][*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 financial institutions such as banks. In light of these developments, to promote private-sector innovation and ensure appropriate user protection, etc., 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 services, etc., are entities that, on behalf of banks etc., uses electronic data processing systems to reduce the volume of deposit claims equivalent to the transferred funds or to increase the volume of deposit claims equivalent to the funds received through exchange transactions with depositors, etc. who have opened deposit accounts with banks, etc.
Due to being designated as specific business operators under the Act on Prevention of Transfer of Criminal Proceeds, electronic payment handling service providers, etc., 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 money from users. Furthermore, the users of electronic payment handling services, etc., 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 reduced to a level comparable to the services provided by deposit-taking institutions.

(ii) Trends of STRs

The number of STRs submitted by deposit-taking financial institutions from 2020 to 2022 was 1,189,637 cases, accounting for 77.0% of the total reports.

The Financial Services Agency revised the "List of Reference Cases of Suspicious Transactions"[*3] for deposit-

---

* [1]Electronic payment handling services, 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).

* [3]Competent authorities provide *the List of Reference Cases of Suspicious Transactions* to specified business operators. The list illustrates patterns that specified business operators should pay especially close attention to because they could indicate suspicious business transactions. When specified business operators submit STRs, they are required to state which reference case the transaction mainly falls under.

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.

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

Table 31: Reporting Status of Major STRs by Deposit-Taking Financial Institutions

Reason for reporting	Number of reports	Percentage (%)
43. Customers with unusual behavior or movements	272,260	22.9
42. Transactions related to Boryokudan gangsters or their parties	143,390	12.1
14. Frequent remittances from numerous individuals	107,597	9.0
27. Large remittances from/to other countries for economically unreasonable purposes	72,954	6.1
16. Sudden large deposits, withdrawals and remittances	71,748	6.0
1. Large cash transactions	60,862	5.1
11. Frequent large deposits, withdrawals and remittances	49,699	4.2
44. Unusual transactions based on the purpose, occupation or content of business	46,415	3.9
5. Transactions under fictious or other party's name	36,416	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 content of these reports, based on suspicions of transactions involving fictitious or borrowed names, includes the following:

- ○ Multiple users with different names and birthdates have attached the same photograph to their identity verification documents.
- ○ Multiple account openings and user registrations have been made from the same IP address.
- ○ Despite the user's country of residence being Japan, the login activity occurred from outside Japan.
- ○ The same mobile phone number was registered for multiple accounts and user contact details, even though the number is 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 financial institution or branch. Additionally, similar applications occur simultaneously.

(iii) Measures to Mitigate Risks

(A) Statutory measures

In order to implement AML/CTF, each relevant law and regulation contains provisions on measures to mitigate risks. The main relevant laws and regulations are as follows:

○ Act on Prevention of Transfer of Criminal Proceeds:

Specified business operators are obligated to perform customer verification and other measures during transactions. In addition, in December 2022, the Act on Prevention of Transfer of Criminal Proceeds was amended, stipulating that specified business operators must notify other specified businesses operators or foreign-exchange transaction operators when conducting foreign exchange transactions, etc. of information not only about customers but also about the recipients of payments.

○ Banking Act

Stipulates that the Financial Services Agency has the right to collect reports from, conduct on-site inspection of, and issue improvement orders against banks as necessary.

* [1]National Police Agency. Seventh Revised Edition (Revised August 2023)

(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.

[Guidelines Established by Competent Authorities, etc.]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism	https://www.fsa.go.jp/common/law/amlcft/211122_en_amlcft_guidelines.pdf (Financial Services Agency)
Frequently Asked Questions Regarding " Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism"(FAQ)	https://www.fsa.go.jp/common/law/amlcft/en_amlcftgl_faq.pdf (Financial Services Agency)
Comprehensive Guidelines for Supervision for Major Banks, etc.	https://www.fsa.go.jp/common/law/guide/city/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision for Small, Medium-Sized, and Local Financial Institutions, etc.	https://www.fsa.go.jp/common/law/guide/chusho/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 in 2022]
<Financial Services Agency>
- Revised the "Frequently Asked Questions (FAQs)" on the Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism (August 2022).
- 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>
- 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 Countering the Financing of Terrorism in collaboration with the Financial Services Agency (about 680 cases) (March 2022).
- Exchanged opinions on each service with persons in charge at all prefectural governments, regional agricultural administration offices, and industry associations, etc.
- Conducted inspections focused on compliance with the Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism and institutional preparations for the inspected entities, including a risk-based approach.

<Ministry of Health, Labour, and Welfare>
- Collaborated with the Financial Services Agency to conduct inspections based on guidelines such as the Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism.
- Participated in joint inspections with the Financial Services Agency, sharing inspection methods, perspectives, and other insights. Also, received training related to the Financial Services Agency's anti-money laundering efforts.

(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, offering training, etc. In particular, the Japanese Bankers Association (JBA) continuously follows up on the FATF's considerations on AML/CFT measures.

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 in 2022]
<Industry Association>
- Established the Cooperation Agency for Anti-Money Laundering with the aim of advancing and collaborating on ML/TF prevention efforts (January 2022, Japanese Bankers Association).

< 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 crypto-assets, some deposit-taking financial institutions have taken measures to verify the ML/TF risk management capabilities of crypto-assets exchange service providers. These measures include issuing questionnaires and providing the capability for crypto-assets exchange service providers to suspend the use of dedicated deposit accounts in cases of detected misuse.

[Emergency Countermeasures Plan for Robbery and Online and Telephone Fraud Cases Using the Method of Recruiting Perpetrators on Social Media] (Excerpt)
As mentioned in *Section 3: Analysis of Money Laundering Cases, etc.*, of this NRA-FUR, considering the frequent occurrence of online and telephone fraud cases in Japan, the Crime Countermeasures Ministerial Meeting was held on March 17, 2023. During this meeting, the Emergency Countermeasures Plan for Robbery and Online and Telephone Fraud Cases Using the Method of Recruiting Perpetrators on Social Media was formulated. Two measures related to deposit-taking financial institutions were outlined, and the National Police Agency and the Financial Services Agency have been discussing and promoting initiatives based on this plan. To further enhance countermeasures, a collaborative effort between the government and the private sector is being undertaken through discussions with deposit-taking financial institutions and their industry associations.
(Excerpt from the plan)
2. Measures to Eradicate Tools that Facilitate Execution
(4) Strengthening Measures to Prevent the Illicit Use of Deposit/Savings Accounts
Given the observed phenomenon of illicitly transferred deposit/savings accounts being utilized within crime groups for financial transactions and other purposes, for enhancement of customer management related to deposit/savings accounts and, preventing their misuse. Discussions involving industry associations and other stakeholders are being conducted to promote measures such as strict transaction verification at the time of using deposit/savings accounts as required by the Act on Prevention of Transfer of Criminal Proceeds and increased communication and awareness-raising by financial institutions towards their customers.
Additionally, to ensure the effectiveness of personal identification as mandated by the Act on Prevention of Transfer of Criminal Proceeds and similar laws, proactive utilization of the public personal authentication function of the Individual Number Card in non-face-to-face identity verification is being promoted, including potential system revisions.
(7) Prevention of Unauthorized Transfer of Mobile Phones and Deposit/Savings Accounts by Returning Resident Foreign Nationals
2) Prevention of Unauthorized Transfer of Savings Accounts
There is an observed reality where deposit/savings accounts illicitly transferred from resident foreign nationals returning to their home countries are being utilized for criminal activities. To prevent such deposit/savings accounts from being inappropriately used, ongoing public relations and awareness campaigns will be conducted. Additionally, measures such as strengthening the management of deposit/savings accounts based on the period of stay and discussions involving industry associations will be promoted to ensure that crime groups or other entities do not misuse deposit/savings accounts by impersonating these foreign nationals.
Furthermore, aiming to prevent the misuse of their services, establishing a shared information system for financial institution to facilitate the smooth confirmation of the period of stay for resident foreign nationals will be considered.

Source: Prime Minister's Office Website

(iv) Assessment of Risks

Deposit-taking institutions provide various products and services, including accounts that guarantee safe fund management, deposit transactions for quick 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 money laundering[*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 so on, the risk of misuse for money laundering is considered to be relatively high in comparison with other types of businesses. Competent authorities and specified business operators are taking the above-mentioned mitigating measures against these risks, in addition to statutory measures, and the outcomes of such measures can be seen from the effective efforts made by deposit-taking institutions.

However, these efforts differ from one deposit-taking institution to another. Deposit-taking institutions that are 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. Most of the modus operandi used for cleared cases of concealment of criminal proceeds in 2022 involved deposits into accounts under the names of fictious or other parties. There were more than a dozen accounts under the names of fictious 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 fictious or other parties' names are the main criminal infrastructure of ML/TF, among others. Deposit-taking institutions that provide the accounts must take continuous measures to prevent the transfer of accounts and subsequently detect illegal transactions.

In addition, in light of cases where products or services provided by deposit-taking institutions were misused for money laundering, 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, fictitious, borrowed, or 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, business contents, etc.
○ Transactions involving deposits and withdrawals using the accounts of customers who have multiple accounts (including accounts held under different names using store names, etc.)

[Cooperation between Financial Institutions on Transaction Monitoring, etc.]
In light of the digitization of finance and the sophistication of the modus operandi of ML/TF, etc., 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 banks that do not implement appropriate measures are generally at risk of ML and other offences.

---

* [1] Article 2, paragraph 2, item 28 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 36 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.

Considering this situation, efforts are being made to enhance and streamline the core operations of AML/CFT in financial institutions, such as joint filtering and 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, provides for the establishment of a system related to funds transfer transaction analysis provider that undertake assignments from multiple deposit-taking institutions, among others, to implement funds transfer transactions. It introduces a licensing system and subjects these entities to inspections and supervision by the Financial Services Agency and other administrative agencies.

- ○ Transaction filtering (to analyze whether customers, etc., are subject to sanction and notify the results of the analysis to deposit-taking institutions, etc.); and
- ○ Transaction monitoring (to analyze whether transactions are suspicious and notify the results of the analysis of deposit-taking institutions, etc.)

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

At Cooperation agency for Anti-Money Laundering established by the Japanese Bankers Association, the following specific services are envisaged:

(1) AI scoring service for transaction monitoring, which scores the risk level of alerts generated by each bank's system.
(2) Provision of operational enhancement support services, which organize and share leading practices and practical case studies on common industry issues

Furthermore, in line with the government's action plan targeting the spring of 2024, preparations are underway for a phased service provision, with the expectation of establishing an effective system that comprehensively captures risks across the entire financial system network.

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

(i) Factors that Increase Risks

(A) Characteristics

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, etc., 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.

As of the end of March 2023, 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.

(B) Typologies

The following case is an example of misusing insurance products for money laundering:

○ A drug trafficking organization spent its drug proceeds on the purchase of life insurance, then canceled the insurance and received a refund soon afterward (case in a foreign country).

The following case is an example of changing the form of criminal proceeds:

○ 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 money laundering:

○ 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

The number of STRs submitted by insurance companies, etc., between 2020 and 2022 was 10,032 (8,453 reports for life insurance, 1,538 reports for non-life insurance, and 41 reports for mutual aid business).

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 32: Reporting Status of Major STRs by Life Insurance

*1 Insurance companies, etc. mean those listed in Article 2, paragraph 2, item 8 (agricultural cooperatives), item 9 (federations of agricultural cooperatives), item 17 (insurance companies), item 18 (foreign insurance companies, etc.), item 19 (small-claim/short-term insurance business operators), and item 20 (mutual aid federation of fishery cooperatives) of the Act on Prevention of Transfer of Criminal Proceeds.

Reason for report	Number of reports	Percentage (%)
28. Transactions related to Boryokudan gangsters or their parties	6,580	77.8
29. Customers with unusual behavior or movements	181	2.1

Table 33: Reporting Status of Major STRs by General Insurance

Reason for report	Number of reports	Percentage (%)
28. Transactions related to Boryokudan gangsters or their parties	566	36.8
29. Customers with unusual behavior or movements	86	5.6
5. Transactions under fictious or other party's name	57	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. The main relevant laws and regulations are as follows:

○ 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, etc., 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.

[Guidelines Established by Competent Authorities, etc.]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism	https://www.fsa.go.jp/common/law/amlcft/211122_amlcft_guidelines.pdf (Financial Services Agency)
Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism"(FAQ)	https://www.fsa.go.jp/news/r4/202208_amlcft_faq/202208_amlcft_faq.pdf (Financial Services Agency)
Comprehensive Guidelines for Supervision for Insurance Companies	https://www.fsa.go.jp/common/law/guide/ins/index.html (Financial Services Agency)
Guidelines for Supervision for Small-Amount and Short-Term Insurance Companies	https://www.fsa.go.jp/common/law/guide/syougaku/index.html (Financial Services Agency)
Comprehensive Guidelines for Supervision for Authorized Specified Insurers	https://www.fsa.go.jp/common/law/guide/ninka/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 in 2022]
<Financial Services Agency>
• Revised the Frequently Asked Questions (FAQ) regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism". (August 2022)

- Provided lectures and training to other ministries and agencies, industry associations, specified business operators and oversea 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 Countering the Financing of Terrorism in collaboration with the Financial Services Agency. (2 cases). (March 2022)
- 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 Countering 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, etc., 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 in 2022]

- Based on the policy for the fiscal 2022 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 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 2022 compliance program, provided training on and raised awareness of the Fishery Cooperative Association regarding establishment of basic policies on compliance for officers and employees, more effective promotion of compliance in daily business operations, and measures including verification of identity and other information (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) Assessment of Risks

Since insurance products with cash accumulation features enable criminal proceeds to be converted to immediate or deferred assets, they can be a useful measure of ML/TF.

Actually, there are cases where money laundering 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.

Competent authorities and insurance companies, etc., 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, etc., 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.

In light of cases where insurance products were misused for money laundering, 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, fictitious, borrowed, or 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.

(3) Products and Services, etc. Dealt with by Financial Instruments Business Operators, etc., and Commodity Derivatives Business Operators[*1]

(i) Factors that Increase Risks

(A) Characteristics

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 2023, there were 5,402 financial instrument business operators registered by the Prime Minister or those notified to the Prime Minister based on the Financial Instruments and Exchange Act (Act No. 25 of 1948). 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 36.

Upon reviewing the trading conditions of stocks and commodities as investment targets in Japan, the total transaction value[*2] of stocks listed on the Tokyo Stock Exchange in 2022 was about 606 trillion yen in the Prime Market, about 16 trillion yen in the Standard Market, and about 25 trillion yen in the Growth Market.

For commodity derivative transactions, the trading volumes amounted to approximately 2.49 million sheets[*3] at the Tokyo Commodity Exchange and the Dojima Commodity Exchange in 2022.

Investment has different characteristics to deposit/savings; customers risk losing principal when the market price of the investment targets fluctuates. However, at the same time, they can obtain more profit than with deposit/savings if the investment succeeds.

From the perspective of the risk of abuse for ML/TF, it will be difficult to track criminal proceeds if criminals deposit funds, sell or purchase stocks, or conduct commodity derivative transactions, and convert a large amount of money into various commodities or make investments in financial products with a complicated structure and make the source of the funds unclear.

Financial instruments business operators, etc. 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, according to the Financial Services Agency. Therefore, there is a risk of transferring criminal proceeds through these transactions. For example, when providing deposit and withdrawal services linked to group's bank accounts, there is a risk that the necessary confirmations will be insufficient due to the acceleration of fund transfers. Furthermore, there is a risk that insider trading will be conducted, and the funds obtained from insider trading will be combined with legal assets, or that the sale and purchase of stocks will be used to raise funds for Boryokudan, etc. In non-face-to-face transactions, there is a risk of dealing with a fictitious person or a person impersonating another person.

(B) Typologies

The following cases are common examples of products and services dealt with by financial instruments business

---

*1 Meaning the persons listed in Article 2, paragraph 2, item 21 of the Act on Prevention of Transfer of Criminal Proceeds (financial instruments business operators), persons listed in item 22 of the same paragraph (securities finance companies), persons listed in item 23 of the same paragraph (notifiers of specially permitted services), persons listed in item 24 of the same paragraph (notifiers of specially permitted services for foreign investors, etc.) and persons listed in item 33 of the same paragraph (commodity derivatives business operators).

*2 The figures for 2022 do not include the values from January 4 through April 1st.

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

operators, etc., and commodity derivatives business operators, as well as brokerage services for commissioned transactions on commodity markets that were misused for money laundering:

○ 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

The numbers of STRs submitted by financial instrument business operators, etc., and commodity derivatives business operators between 2020 and 2022 were 56,683 and 1,026, respectively.

The Financial Services Agency, Ministry of Agriculture, Forestry and Fisheries, and Ministry of Economy, Trade and Industry have published a 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 the financing of terrorism, 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 34: 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	14,023	24.7
38. Customers with unusual behavior or movements	12,947	22.8
37. Transactions related to Boryokudan gangsters or their related parties	7,406	13.1

Table 35: 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	758	73.9

(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. The main relevant laws and regulations are as follows:

○ Financial Instruments and Exchange Act and Commodity Futures 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, etc., for industry associations and specified business operators.

[Guidelines Established by Competent Authorities, etc.]

Name of Guidelines, etc.	Website's URL, etc.

Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism	https://www.fsa.go.jp/common/law/amlcft/211122_en_amlcft_guidelines.pdf (Financial Services Agency)
Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism"(FAQ)	https://www.fsa.go.jp/common/law/guide/kinyushohin_eng.pdf (Financial Services Agency)
Comprehensive Guidelines for Supervision for Financial Instruments Business Operators, etc.	https://www.fsa.go.jp/common/law/guide/kinyushohin/index.html (Financial Services Agency)
Basic Guidelines for Commodity Derivatives Business Operators, etc.	https://www.maff.go.jp/j/shokusan/syoutori/dealing/attach/pdf/hourei-3.pdf (Ministry of Agriculture, Forestry and Fisheries) https://www.meti.go.jp/policy/commerce/z00/190814sakimono-shishin.pdf (Ministry of Economy, Trade and Industry)
Guidelines for Anti-Money Laundering and Countering 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/f00/211019amlcft_guideline.pdf (Ministry of Economy, Trade and Industry)
Points to consider for supervision of specified joint real estate enterprises	https://www.mlit.go.jp/common/001390608.pdf (Ministry of Land, Infrastructure, Transport and Tourism)

[Examples of Initiatives Taken by Competent Authorities in 2022]
<Financial Services Agency>
- Revised the Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism"(FAQ). (August 2022)
- 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 briefings on the revisions and points to note in the Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism in the Commodity Derivatives Business. (May 2022)

<Ministry of Land, Infrastructure, Transport and Tourism>
- Participated as a speaker in compliance training sessions for members organized by industry associations, explaining the importance of measures against money laundering.
- 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 (78 cases). (March 2022)

(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, etc. Financial instruments business operators and commodity derivatives business operators themselves also take measures to establish and strengthen their AML/CFT internal control systems. For example, they set up a division in charge, develop their own rules and manuals, carry out periodic trainings, conduct internal audits, identify transactions that are likely to pose ML/TF risks, and rigorously conduct CDD.

[Examples of Initiatives Taken by Industry Associations in 2022]
- Conducted hearings on the management systems for anti-money laundering and countering the financing of terrorism as part of the written survey items targeting regular member investment management businesses (investment trust management companies and asset management companies), performed risk assessments based on responses from each company, and utilized this information for on-site inspections of the members (The Investment Trusts Association).
- Utilized online platforms to implement training for members (Japan Investment Advisers Association, Japan Securities Dealers Association, and Type II Financial Instruments Business Operator).
- Carried out surveys by using the "Questionnaire on the Status of Compliance with Self-regulatory Rules," which includes questions about efforts made by members to implement AML/CFT for the purpose of self-assessment by the members themselves, and provided information return and alerts to members about the

results, including the status of responses to the Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism (Japan Investment Advisers 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) 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, etc., and increase such obtained rights, etc., 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 money laundering.

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].

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. 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.

---

*1 Article 2, paragraph 2, item 27 of The Act on Prevention of Transfer of Criminal Proceed lists joint real estate enterprises as specified business operators. 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 34 and 35 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, etc., and account management institutions, which open accounts for the book-entry transfer of bonds, etc. for others (which can be performed by securities companies, banks, etc.), 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, real estate, etc., as a fundamental part of the Japanese financial system's infrastructure.

Those who intend to operate a trust business as a trust company must obtain registration, a license, or authorization from the competent authorities based on the Trust Business Act (Act No. 154 of 2004). When banks and other financial institutions operate a trust business, they are required to obtain approval from the competent authorities under the Act on Engagement in Trust Business Activities by Financial Institutions (Act No. 43 of 1943). As of the end of March 2023, 96 business operators were engaging in trust business with such a license and authorization.

No cleared money laundering case involving the misuse of trusts has been reported in Japan in recent years. However, 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. Furthermore, by converting a property to a trust beneficiary right, the attribution and quantity of the property, as well as the nature of the property right, can be altered pursuant to the purpose of the trust. From these aspects, a trust can be a useful method for money laundering.

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 above assets 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 according to 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.

(ii) Trends of STRs

There were 72 STRs[*2] related to trusts from 2020 to 2022. Among cases listed as examples in the List of Reference Cases of Suspicious Transactions, the major ones by 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, 38.9%).
- ○ Transactions related to Boryokudan gangsters or their related parties (17 reports, 23.6%).

(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. The relevant laws and regulations are as follows:

---

*1 Refers to the person listed in Article 2, paragraph 2, item 25 of the Act on Prevention of Transfer of Criminal Proceeds (trust company), the person listed in item 26 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.

○ 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, etc. for industry associations and specified business operators.

[Guidelines Established by Competent Authorities, etc.]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism	https://www.fsa.go.jp/common/law/amlcft/211122_amlcft_guidelines.pdf (Financial Services Agency)
Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism"(FAQ)	https://www.fsa.go.jp/news/r4/202208_amlcft_faq/202208_amlcft_faq.pdf (Financial Services Agency)
Comprehensive Guidelines for Supervision for Trust Companies, etc.	https://www.fsa.go.jp/common/law/guide/shintaku/index.html (Financial Services Agency)

[Examples of Initiatives Taken by Competent Authorities in 2022]
<Financial Services Agency>
- Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism" (FAQ). (August 2022)
- 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).
- Provided lectures and training to other ministries and agencies, industry associations, and specified business operators to improve AML/CFT.

(C) Measures by industry associations and business operators

Industry associations support the AML/CFT measures taken by each trust company by providing training and a range of information from external consulting companies through business communication meetings and study-group meetings on money laundering. The Association explains to each member company the details to be described in the documents to be prepared by specified business operators and points for verification according to the intention of each trust 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 in 2022]
- 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) 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 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 money laundering 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 etc. to another, and trust companies, etc., 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) Characteristics

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, etc. 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, etc., and the expansion of transactions through the Internet, money-lending services have become more convenient.

By taking advantage of such convenience, those who obtained criminal proceeds can make it difficult for the authorities to track their criminal proceeds by misusing money lending, such as lending and repaying money repeatedly.

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 2023, there were 1,548 registered business operators, while the outstanding balance of loans was 36.9641 trillion yen at the end of March 2023.

(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 money laundering.

○ A criminal used a forged image of other person's driver's license to open a bank account in the name of fictious or other party and applied for a loan contract with a money lender on the Internet to have the money lender deposit the loan into the account.

(ii) Trends of STRs

The number of STRs submitted by money lenders, etc., was 106,381 between 2020 and 2022.

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 36: Reporting Status of Major STRs by Money Lenders

Reason for report	Number of reports	Percentage (%)
43. Customers who show unusual behavior or movements	39,972	37.6
5. Transactions in a fictious or other party's name	28,917	27.2

(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, and each relevant law and regulation contains provisions on measures to mitigate risks. The main relevant laws and regulations are as follows:

*1 Money Lenders, etc. mean those listed in Article 2, paragraph 2, item 29 (money lender) and item 30 (short-term credit broker) of the Act on Prevention of Transfer of Criminal Proceeds.

○ 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, etc., 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.

[Guidelines Established by Competent Authorities, etc.]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism	https://www.fsa.go.jp/common/law/amlcft/211122_amlcft_guidelines.pdf (Financial Services Agency)
Frequently Asked Questions Regarding " Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism"(FAQ)	https://www.fsa.go.jp/news/r4/202208_amlcft_faq/202208_amlcft_faq.pdf (Financial Services Agency)
Comprehensive Guidelines for Supervision for Money Lenders	https://www.fsa.go.jp/common/law/guide/kashikin/index.html (Financial Services Agency)

[Examples of Initiatives Taken by Competent Authorities in 2022]
<Financial Services Agency>
- Revised the Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism" (FAQ). (August, 2022)
- Provided lectures and training to other ministries and agencies, industry associations, and specified business operators 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, etc., 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 Associations>
- Conducted training sessions for lenders aimed at establishing systems required by the Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism (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) 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, etc., 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.

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 etc. to another, and money lenders, etc., taking ineffective 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.

In addition, based on the cases where money lenders were misused for money laundering, etc., 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.

(6) Funds Transfer Services Dealt with by Funds Transfer Service Providers

(i) Factors that Increase Risks

(A) Characteristics

A funds transfer service means an exchange transaction service (registration, etc., of the appropriate remittance type, etc., 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, etc., 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 2023, there were 84 registered business operators. There were 1,548.78 million remittances totaling 5,467.8 billion yen in fiscal 2021. 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 37).

Table 37 Trends in Funds Transfer Service Business

Category \ Year		2019	2020	2021
Number of remittances per year		454,597,616	963,073,667	1,548,782,833
Breakdown	Domestic	404,901,313	892,640,092	1,473,790,829
	Cross-border	49,696,303	70,433,575	74,992,004
Transaction volume per year (million yen)		2,307,847	3,995,550	5,467,864
Breakdown	Domestic	1,180,007	2,595,589	3,989,725
	Cross-border	1,127,837	1,399,956	1,478,134
Number of registered funds transfer service providers		75	80	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 and depositing it into a bank account. Various business models are being developed, and risks exist in different areas for each funds transfer service provider, depending on the various services that each provider is developing. For example,

---

*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.

one provider has developed a system that allows international funds transfer without using the remittance network of deposit-taking institutions, and developed services based on its own unique method of funds transfer. 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 form a convenient system for providing a quick and secure way to transfer funds on a global scale with reasonable fees. However, these services also facilitate ML/TF by allowing the transfer of funds to foreign countries where legal or transaction systems are different from those of Japan, and it is harder to trace criminal proceeds.

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 develop a system that can handle the risks corresponding to its transaction amount, business scale, and characteristics appropriately. Since some funds transfer service providers do not verify customers' identity and other information appropriately and are unable to examine the risks related to customer attributes, etc., comprehensively and specifically due to inaccurate customer information, they do not conduct risk assessment based on specific and objective information that can be obtained from analysis of STRs, etc. or otherwise do not make such efforts in a timely manner, the Financial Services Agency considers it necessary for funds transfer service providers to comprehensively and specifically to identify and assess the risks based on the scale and characteristics of their business operations. Furthermore, 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.

[Threats and Vulnerabilities, etc. 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, etc., in compliance with the laws and regulations of Japan, etc.
- 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 money laundering:

○ A person was asked to cross-border remittance for a reward, and the person did it through a funds transfer service provider even though they knew that there was no justifiable reason for it (money mule[*1] case).

○ A dangerous drugs trafficker concealed his proceeds in an account opened in fictious or other party's name, and then paid for the procurement of materials to produce drugs from overseas using funds transfer services.

○ An offender transferred proceeds from selling fake brand goods to an account under the name of a relative using funds transfer services.

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

○ A person who was leasing a room in a building received proceeds from gambling played in the room in the name of rent 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 the leader of 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.

In the past, there were cases where an offender transferred criminal proceeds derived from illicit transfers involving Internet banking to another account and then conducted a Money Mule by which funds were transferred to foreign countries by misusing funds transfer services.

(ii) Trends of STRs

The number of STRs submitted by funds transfer service providers was 36,810 between 2020 and 2022.

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 38: Reporting Status of Major STRs by Funds Transfer Services

Reason for report	Number of reports	Percentage (%)
44. Unusual transactions based on the purpose, occupation or content of business	8,577	23.3
15. Sudden large deposits, withdrawals and remittances	4,465	12.1
42. Transactions related to Boryokudan gangsters or their related parties	2,804	7.6
16. Economically unreasonable transactions	1,615	4.4
4. Transactions under fictious or other party's name	1,143	3.1

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. The main relevant laws and regulations are as follows:

○ 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, etc. for industry associations and specified business operators.

[Guidelines, etc. Established by Competent Authorities]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism	https://www.fsa.go.jp/common/law/amlcft/211122_amlcft_guidelines.pdf (Financial Services Agency)
Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism"（FAQ）	https://www.fsa.go.jp/news/r4/202208_amlcft_faq/202208_amlcft_faq.pdf (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/14.pdf (Financial Services Agency)

[Examples of Initiatives Taken by Competent Authorities in 2022]
<Financial Services Agency>
- Revised the Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism"（FAQ）. (August 2022)
- Conducted briefing sessions through industry associations in October 2022, focusing on the key points of the FAQ Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism" revised in August 2022, and the necessity of developing risk management systems for money transfer business operators facing related risks.
- Implemented a partial revision of the Administrative Guidelines (Third Volume: Financial Companies) (Section 14 related to money transfer business operators), addressing unregistered operators (those engaged in currency exchange business without obtaining the license required under the Banking Act or the registration required under the Payment Services Act).(October 7, 2022)
- Provided lectures and training for other ministries and agencies, industry associations, and specified business operators to improve AML/CFT

(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. 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 Industrial Associations in 2022]
- 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, charge 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 (the Japan Payment Service Association).

(iv) 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 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 overseas 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 (recharging) 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.

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.

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.

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, and providers taking ineffective 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.

Considering the cases where funds transfer service providers were misused for money laundering, 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 names, 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

(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:

- ○ So-called stablecoins have vulnerabilities to being exploited for ML/TF, similar to Crypto-assets, 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 stablecoins are more stable in value compared to existing crypto assets, 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[*3] transactions can easily occur, posing a significant vulnerability to money laundering.
- ○ To mitigate the risks associated with so-called stablecoins, their issuers and intermediaries should bear obligations for ML/TF measures similar to those of financial institutions and crypto-assets exchange service providers.
- ○ So-called stablecoins can become globally available quickly and circulate across multiple jurisdictions, making international cooperation essential to address money laundering risks adequately.

Although the issuance of electronic payment instruments has not been confirmed in Japan as of the end of September 2023, 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, including globally, and technological advancements.

---

*1 Entities listed in Article 2, Paragraph 2, Subparagraph 31-2 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).

*3 Peer to Peer

(ii) Measures to Mitigate Risks

(A) Statutory measures

In order to implement AML/CTF, each relevant law and regulation contains provisions on measures to mitigate risks. The main relevant laws and regulations are as follows:

○ Act on Prevention of Transfer of Criminal Proceeds

In June 2022, the Act on Prevention of Transfer of Criminal Proceeds was amended to include electronic payment transaction services as specified business operators. In addition to various obligations such as conducting verification at the time of transactions, creating and preserving verification records, and STRs, electronic payment transaction services are required to ensure that foreign-based electronic payment transaction services with which they continuously or repeatedly transfer electronic payment instruments have established a system capable of properly conducting measures equivalent to verification at the time of transactions.

Furthermore, in December of the same year, it was stipulated that when electronic payment instruments service providers transfer electronic payment instruments, they must notify other electronic payment instruments service providers or foreign electronic payment instruments service providers of information regarding the customer as well as 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.

(B) Measures by competent authorities

[Guidelines, etc. Established by Competent Authorities]

Guideline name, etc.	Website URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism	https://www.fsa.go.jp/common/law/amlcft/211122_amlcft_guidelines.pdf (Financial Services Agency)
Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism"（FAQ）	https://www.fsa.go.jp/news/r4/202208_amlcft_faq/202208_amlcft_faq.pdf (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/18.pdf (Financial Services Agency)

(iii) Assessment of Risks

Electronic payment instruments, similar to Crypto-assets due to their technological similarities, such as the potential use of distributed ledger technology, are recognized to 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 Crypto-assets 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, including global 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 crypto-asset 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 crypto-assets 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, etc., to new entrants that have not implemented appropriate ML/TF countermeasures, indicating the need for continuous measures to reduce risks.

(8) Crypto-assets Dealt with by Crypto-assets Exchange Service Providers

(i) Factors that Increase Risks

(A) Characteristics

In Japan, under the Payment Services Act, crypto-assets 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 crypto-assets exchange service business must be registered by the Prime inister based on the Payment Services Act. As of the end of June 2023, there are 30 registered business operators.

The transaction amounts in crypto-assets are increasing globally, including in Japan, and, as a result, the number of cleared cases involving crypto-assets is rising. July 2019 saw cases where huge amounts of crypto-assets seemed to be illicitly transmitted from domestic crypto-assets exchange service providers. It is considered that these cases occurred because new crypto-assets exchange service providers did not have an appropriate internal control system that corresponds to each type of risk, including cyber security risks, and also because of continuing challenges of security threats in cyberspace. For example, the number of cleared cases of cybercrimes in 2022 was a record high of 12,369 cases, loss from ransomware increased, and information leaks caused by illegal access and cyber-attacks by cyber-attack groups supported by national governments occurred. On the other hand, since the Payment Services Act amendment in May 2019, which mandated the segregation of customer assets (management in cold wallets not connected to the network), no incidents of customer asset leakage due to cyber-attacks on crypto-assets exchange service providers have occurred since the enforcement of the amended law in May 2020.

In most crypto-assets have characteristics in which their transfer history is published on the blockchain, so their transactions can be traced. However, there are various designs and specifications for crypto-assets. Among the crypto-assets used for transactions by crypto-assets exchange service providers, one is known to not disclose transfer records, making it difficult to trace transactions, so it is likely to be used for ML/TF. Another is known to be poor at maintaining and updating its transfer records.

Recently, technologies that increase the anonymity of crypto-assets transactions include:

- ○ “Peel chains,” which involve transferring small amounts of crypto-assets 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 crypto assets.
- ○ “Chain hopping,” which involves moving crypto-assets from the blockchain it is recorded on to another blockchain.

The use of these technologies can obscure the trail of crypto-assets transfers, making tracking difficult. In the United States, sanctions have been implemented against companies providing mixing services for assisting in the money laundering of criminal proceeds.

If wallets used for transactions are acquired or controlled by individuals or crypto-assets exchange service providers who exist in countries or areas where they are not obliged to take measures to conduct identity verification, etc., it becomes difficult to identify the owner of the crypto-assets transferred in a transaction. Since almost all transactions handled by crypto-assets exchange service providers are not conducted in person but over the Internet, they have high anonymity.

With respect to the exchange of crypto-assets and legal currencies, there are crypto ATMs where crypto-assets and legal currencies can be exchanged in some foreign countries. This makes it possible to get crypto-assets cashed or to purchase crypto-assets with cash and improve the convenience for users. Since there are cases overseas in which drug traffickers convert criminal proceeds derived from drug trafficking into bitcoins via crypto ATMs using forged identification documents, it is necessary to see how such ATMs are actually being used.

[Threats and Vulnerabilities, etc. Found by Competent Authorities in Recent Years]
- It has been observed that crypto-assets 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 crypto-asset transactions were not detected because the effectiveness of transaction monitoring scenarios had not been examined. This resulted in overlooking the implementation of a scenario with specifications that differed from the development requirements.

(B) Typologies

The following cases are common examples of misusing crypto-assets for money laundering:

○ An offender purchased crypto-assets through an unregistered crypto-assets exchange service provider to disguise the purchase as asset management of funds stolen through FX transaction fraud and received the funds at an address managed by the offender so they could be withdrawn in cash.

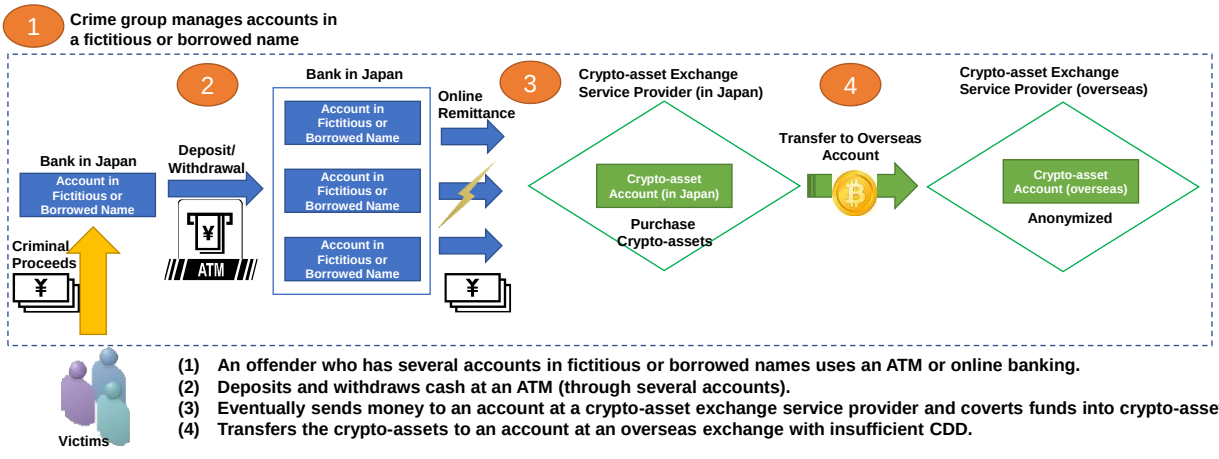
○ An offender moved crypto-assets obtained through computer fraud to an account at an overseas crypto-assets exchange provider that could be opened in an anonymous name.

○ An offender made an employee of a company engaging in transactions for crypto-assets purchase crypto-assets using criminal proceeds that were transferred to an account in the company's name and made the employee convert the crypto-assets into cash by transferring the crypto-assets to a crypto address managed by the offender and returning almost the same amount of crypto-assets to the crypto address of the company.

○ As part of bankruptcy proceedings, the required crypto-assets were transferred to the address of a foreign crypto-assets exchange service provider. Then, the crypto-assets obtained through trading these assets were transferred to the address of another crypto-assets exchange service provider.

○ Criminal proceeds obtained through fraud were used to purchase crypto-assets, which were then transferred to the address of a foreign crypto-assets exchange service provider controlled by the perpetrators.

Table 39: [Flow of Money Laundering Involving Abuse of Crypto-Assets]



(1) An offender who has several accounts in fictitious or borrowed names uses an ATM or online banking.
(2) Deposits and withdraws cash at an ATM (through several accounts).
(3) Eventually sends money to an account at a crypto-asset exchange service provider and coverts funds into crypto-assets.
(4) Transfers the crypto-assets to an account at an overseas exchange with insufficient CDD.

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 crypto-assets exchange between a customer and a crypto-assets exchange service provider:

- ○ A case where an offender provided IDs and passwords for crypto-asset transaction 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 crypto-assets exchange service providers using the principal identification documents of a fictitious or other party.

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

- ○ A case where crypto-assets were used to pay for illegal drugs purchased on a website in another country.
- ○ A case where ransomware demanded payment in crypto-assets.
- ○ A case where crypto-assets were used by an unlicensed financial instruments business operator to transact financial instruments.

(ii) Trends of STRs

The number of STRs submitted by crypto-assets exchange service providers between 2020 and 2022 was 38,113. 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 40: Reporting Status of Major STRs by Crypto-assets Exchange Service Providers

Reason for report	Number of reports	Percentage (%)
41. Customers with unusual behavior or movements	5,358	14.1
2. Frequent in a short-term, with large total amount of cash	3,687	9.7
4. Transactions under fictious or other party's name	3,203	8.4
34. Refusal to provide true beneficiary explanations and materials	1,530	4.0
20. Sudden large deposits, withdrawals and remittances	1,335	3.5

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

(iii) Measures to Mitigate Risks

(A) Statutory measures

In order to implement AML/CTF, each relevant law and regulation contains provisions on measures to mitigate risks. The main relevant laws and regulations are as follows:

○ 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 on Prevention of Transfer of Criminal Proceeds was amended in December 2022, crypto-assets exchange service providers are required to ensure that foreign-based crypto-assets exchange service providers with which they continuously or repeatedly transfer crypto assets have established a

system capable of properly conducting measures equivalent to verification at the time of transactions. It also specifies that crypto-assets exchange service providers must inform other crypto-assets exchange service providers or foreign crypto-assets exchange service providers about the customer and the counterparty's information when transferring crypto assets, effective from June 1, 2023.

○ Payment Services Act

Stipulates that the competent authorities have the right to collect reports from, conduct on-site inspection, and issue business improvement orders, etc., against crypto-assets exchange service providers as necessary.

○ FEFTA

Impose the obligation for crypto-assets exchange service provider to identify customers and restricted transactions for asset freezing measures when transferring crypto-assets related to customer payments.

(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.

[Guidelines, etc. Established by Competent Authorities]

Name of Guidelines, etc.	Website URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism	https://www.fsa.go.jp/common/law/amlcft/211122_amlcft_guidelines.pdf (Financial Services Agency)
Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism" (FAQ)	https://www.fsa.go.jp/news/r4/202208_amlcft_faq/202208_amlcft_faq.pdf (Financial Services Agency)
Guidelines for Administrative Work (Third volume: for finance companies 16 for crypto-assets exchange service providers)	https://www.fsa.go.jp/common/law/guide/kaisya/16.pdf (Financial Services Agency)

[Examples of Initiatives Taken by Competent Authorities in 2022]
<Financial Services Agency>
- Revised the Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism" (FAQ) (August 2022)
- Implemented a partial amendment to the Guidelines for Administrative Work (Third volume: for finance companies 16 for crypto-assets exchange service providers) that require measures in accordance with the risk associated with transactions involving the transfer of crypto assets (the so-called "Travel Rule") and transactions with wallets managed by the users themselves (unhosted wallets), effective from June 1, 2023.
- Provided lectures and training to other ministries and agencies, industry associations, and specified business operators to improve AML/CFT
- 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 crypto-assets 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 Countering 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 crypto-assets, etc. In addition, in light of the List of Reference Cases of Suspicious Transactions for crypto-assets 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 crypto-assets exchange service provider has developed and strengthened its internal control system by preparing documents to be prepared by specified business operators, etc., establishing regulations and manuals, identifying high-risk transactions, and strictly monitoring high-risk transitions to implement AML/CFT.

[Examples of Initiatives Taken by Industry Associations and Specified Business Operators in 2022]
<Industry Associations>
- To comply with the Travel Rule related to crypto-assets, which was scheduled for implementation in 2023, self-regulatory rules were revised. Members were informed about the need to acquire additional information, such as "transfer purpose information" and "recipient address information" for crypto-assets (October 2022, Japan Virtual and Crypto Assets Exchange Association).

<Specified Business Operators>
- Some crypto-assets 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 wallet addresses used for illicit withdrawals through blockchain analysis tools, and implementing two-factor authentication during login and deposits/withdrawals.

(iv) Assessment of Risks

Crypto-assets allow users to be anonymous and enable instant cross-border transfers. In addition, some countries have no or inadequate regulation on crypto-assets. If crypto-assets exchange service providers in these countries are abused for crimes, it is difficult to trace the transfer of such crypto-assets. Indeed, there have been cases where offenders abused the anonymity of crypto-assets to change them into cash after moving them through overseas crypto-assets exchange service providers and deposit funds in an account under the name of fictious or other party. For this reason, it is considered that crypto-assets are at risk of misuse for ML/TF. Additionally, it is recognized as a factor that increases risks that, in our country, violations of the Act on Prevention of Transfer of Criminal Proceeds, such as transferring information necessary for the transfer of crypto-assets to other party, are on the rise. 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, customer attributes, etc.

Furthermore, considering that crypto-assets transactions are increasing globally and the environment surrounding such transactions is rapidly changing, it is recognized that the level of risk for misuse of crypto-assets for ML/TF is relatively high in comparison to other types of business.

Although deposit-taking institutions have improved their AML/CFT measures, there are cases where persons who intend to commit ML/TF use crypto-asset transactions in addition to products and services handled by deposit-taking institutions. This situation is increasing the degree of risk associated with crypto assets.

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. They 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 crypto-asset transactions, so crypto-assets exchange service providers need to implement high-level measures in advance. If such measures are not taken sufficiently, crypto-assets exchange service providers will not be able to lower the degree of risk appropriately, and the degree of risk will remain high.

[International Trends in Crypto Assets, etc.]

Since the FATF Recommendation for crypto-assets and crypto-assets 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 report "Virtual Assets: Targeted Update on Implementation of the FATF Standards[*1]," published in June 2023, points out challenges with crypto assets, noting:

- ○ While some jurisdictions have introduced regulations for crypto-assets and crypto-assets exchange service providers, the global implementation of FATF Recommendation 15 on crypto-assets is not satisfactory. Compliance with the standards lags behind most other financial sectors. More than half of the jurisdictions surveyed have not taken measures to implement the Travel Rule, indicating its implementation remains insufficient.
- ○ Although a considerable number of technical solutions exist in the private sector, and some jurisdictions' crypto-assets exchange service providers have started to use them, very few tools fully meet all the FATF standard's Travel Rule requirements, and there are challenges with tool interoperability.

The report also raises serious concerns about the threat of crypto assets illicitly obtained through ransomware attacks or sanction evasion by North Korea being used to fund the proliferation of weapons of mass destruction. Crypto assets increase the risk of terrorist financing for ISIL, AQ, and extremist right-wing groups.

Risks associated with ML/TF in the crypto-asset ecosystem, including decentralized finance (DeFi[*2]) and peer-to-peer (P2P) transactions with unhosted wallets, are highlighted. Sanctioned individuals could exploit these, posing challenges in mitigating these risks. These include identifying natural or legal persons responsible for DeFi structures, assessing risks related to illicit transactions involving unhosted wallets, including P2P transactions, and addressing data gaps in risk assessments. As the crypto-asset ecosystem evolves and crypto-assets exchange service providers implement AML/CTF controls, risks from DeFi and P2P transactions may increase. This trend is likely to become more pronounced as crypto-assets become widely accepted and used for payments without converting to fiat currency.

In February 2023, the FATF announced an agreement on a roadmap to enhance the implementation of FATF standards. By the first half of 2024, it plans to publish measures taken by all FATF member countries and jurisdictions with significant crypto-asset activities to regulate and supervise crypto-assets exchange service providers. Additionally, the FATF and the Virtual Assets Contact Group (VACG) will continue to share insights, experiences, and challenges regarding unhosted wallets, including DeFi and P2P, and monitor market developments in this area to determine if further FATF work is necessary.

In this context, Japan has been closely monitoring changes and emerging ML/TF risks associated with crypto-assets and new technologies surrounding them. In 2023, it published a study on *understanding reality using on-chain/off-chain data in decentralized financial systems*[*3]. The Financial Services Agency's study group on digital and decentralized finance[*4] has been deepening considerations for addressing risks in this field through discussions based on expert information. The study report indicates that determining high risks based solely on on-chain data, such as blockchain transaction records, is challenging. Businesses can potentially narrow down and report suspicious transactions more accurately by analyzing off-chain data linked to KYC information obtained from customers, continuous CDD, and transaction monitoring. The report also suggests that efforts to enhance the reliability of data and data analysis, such as comparing multiple published data and survey results from analysis companies, are necessary to improve data reliability.

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

---

*1 *Virtual Assets: In the Targeted Update on Implementation of the FATF Standards*, crypto-assets are classified as Virtual Assets (VA), and crypto-assets exchange service providers are classified as Virtual Asset Service Providers (VASP).

*2 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."

[3] Joint research in the Financial Services Agency's Blockchain Global Initiative research project.
https://www.fsa.go.jp/policy/bgin/ResearchPaper_qunie2_ja.pdf

*4 Minutes and documents are published on the Financial Services Agency's website.
https://www.fsa.go.jp/singi/digital/index.html

(9) Foreign Currency Exchanges Dealt with by Currency Exchange Operators

(i) Factors that Increase Risks

(A) Characteristics

Many Japanese use foreign-currency exchange to obtain foreign currency when they go overseas 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 41).

Table 41: Transactions by Foreign Currency Exchange Operators

Reporter \ Year		2020				2021				2022			
		Number of Reporters	Number of Transactions	Transaction Amount (Million yen)	Transaction Amount for Each Transaction	Number of Reporters	Number of Transactions	Transaction Amount (Million yen)	Transaction Amount for Each Transaction	Number of Reporters	Number of Transactions	Transaction Amount (Million yen)	Transaction Amount for Each Transaction
Depository Institutions	Megabank (Note 2)	4	37,298	8,962	240	4	12,062	6,738	559	4	43,663	15,781	361
	Local Bank	81	39,687	3,706	93	72	12,560	3,036	242	63	31,131	5,377	173
	Shinkin Bank	85	718	74	103	70	534	65	121	53	1,489	168	113
	Foreign Bank	20	181	59	326	19	232	97	418	20	252	369	1,465
	Other (Note 3)	7	22,848	1,406	62	6	7,465	726	97	6	4,294	662	154
Businesses Other Than Depository Institutions	Funds Transfer Business/ Credit Card Business	6	39,767	3,148	79	11	19,420	5,096	262	9	74,288	17,432	235
	Hotel Business	23	559	39	69	19	65	17	261	18	847	147	173
	Travel Business	16	7,404	381	51	10	149	64	429	12	431	96	223
	Secondhand Articles Dealer Business	40	16,309	1,773	109	36	10,225	1,965	192	42	23,296	3,416	147
	Airport-related Business	3	26,592	998	38	3	6,339	432	68	3	26,610	1,540	58
	Large-scale Retail Business	2	54	2	40	1	13	0.3	25	1	37	1	36
	Other	60	45,136	20,607	457	41	27,500	9,742	352	42	54,966	8,158	148
Total		346	236,553	41,155	174	292	96,564	27,978	290	273	261,304	53,147	203

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 the reduction in foreign visitors to Japan and overseas travelers following the spread of COVID-19. However, a recovery is being observed due to the easing of border control measures related to COVID-19 and the depreciation of the yen.

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 can change the physical form of criminal proceeds and makes it possible to exchange a large number of small-denomination bills for a smaller number of large-denomination bills. In addition, it enables non-face-to-face transactions by using foreign currency delivery and automatic foreign currency exchange machines.

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 (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 money laundering:

- ○ 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.
- ○ An offender exchanged illegally obtained foreign currencies for Japanese yen.
- ○ A drug-trafficking organization used unregistered foreign-currency exchange operators to convert drug proceeds to foreign currency. (case in a foreign country)

(ii) Trends of STRs

The number of STRs submitted by foreign currency exchange operators between 2020 and 2022 was 883.

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 42: Reporting Status of Major STRs by Foreign Currency Exchange Operators

Reason for report	Number of reports	Percentage (%)
3. Frequent transactions in a short term	248	28.1
1. Large cash transactions	186	21.1

(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. The relevant laws and regulations are as follows:

- ○ FEFTA

  Stipulates that the competent authorities have the right to conduct on-site inspection at and issue business improvement orders, etc. 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, etc. for industry associations and specified business operators.

[Guidelines, etc. Established by Competent Authorities]

Name of Guidelines, etc.	Website's URL, etc.
Foreign Exchange Inspection Guidelines	https://www.mof.go.jp/policy/international_policy/gaitame_kawase/inspection/guideline_index.htm (Ministry of Finance)

[Examples of Initiatives Taken by Competent Authorities in 2022]
<Ministry of Finance>
- Implementation of foreign exchange inspections in accordance with the Guidelines for Foreign Exchange Inspections

(C) Measures by industry associations and business operators

Some industry associations that have many members providing foreign-currency exchange services have made voluntary efforts to implement AML/CFT. They have done this by preparing and distributing manuals (templates) for establishing documents to be prepared by specified business operators and internal regulations. Furthermore, they hold regular briefing sessions for members in cooperation with competent authorities and provide support for establishing and reinforcing the internal management of each business operator that exchanges foreign currency.

Foreign-currency exchange operators have prepared documents to be prepared by specified business operators, established regulations and manuals, identified high-risk transactions, strictly monitored high-risk transactions, and made other efforts to establish and improve their internal control systems for implementing AML/CFT.

(iv) 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 overseas 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.

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, and foreign-currency exchange operators taking ineffective 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.

Considering the cases where foreign-currency exchange services were misused for money laundering, 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, customer attributes, etc.:

- ○ 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

(10) Financial Leasing Dealt with by Financial Leasing Operators

(i) Factors that Increase Risks

(A) Characteristics

Financial leasing is dealt with by a financial leasing operator, in the form of contracting with a company etc. (lessee) that intends to obtain machinery, vehicles, etc., 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.

(B) Typologies

No cleared money laundering cases involving misuse of financial leasing have been reported in Japan in recent years. However, there was a case where financial leasing was misused to pay tribute to Boryokudan gangsters. In that case, a person associated with Boryokudan gangsters received goods through financial leasing and allowed a head of the Boryokudan gangsters to use them for a long time.

(ii) Trends of STRs

The number of STRs submitted by financial leasing operators during the period from 2020 to 2022 was 357, and among the guideline numbers and names in the Guidance for Submitting STRs, the ones with the highest number of reports are as follows:

Table 43: 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	206	57.7
8. Empty lease	51	14.3

(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 at the time of transactions, etc. 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 Law (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, etc. for industry associations and specified business operators.

[Examples of Initiatives Taken by Competent Authorities in 2022]
<Ministry of Economy, Trade and Industry>
- Continuously conducted hearings with specified business operators on compliance with the Act on Prevention of Transfer of Criminal Proceeds. (4 companies)
- In response to the publication of the 2022 NRA-FUR, requested the Japan Leasing Association to announce the publication to member companies, which was achieved by the Association. (December 2022)
- Conducted research on compliance with the guidelines by nine business operators not belonging to the Japan Leasing Association to confirm that there is no non-compliance with the guidelines. (January 2022)
- Sent instructors to ML/TF countermeasures training conducted by the Japan Leasing Association, repeatedly requesting the assured implementation of the Act on Prevention of Transfer of Criminal Proceeds and explaining the use of the BO (Beneficial Owner) list system. (March 2022)
- Required the submission of a pledge that demands representatives to pledge the assured implementation of the guidelines, among other things, when leasing companies apply for SME Business Restructuring Subsidy. (March 2022)

(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, etc. Established by Industry Associations]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism in Financial Leasing Business	https://www.leasing.or.jp/guideline.html (Japan Leasing Association)

(iv) Assessment of Risks

Although there were no cleared money laundering 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. 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, and financial leasing operators taking ineffective 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.

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, customer attributes, etc.:

○ 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

(11) Credit Cards Dealt with by Credit Card Operators

(i) Factors that Increase Risks

(A) Characteristics

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, etc., over two months or in a revolving form[*1]. As of the end of March 2023, 249 operators were registered.

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, etc. 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.

(B) Typologies

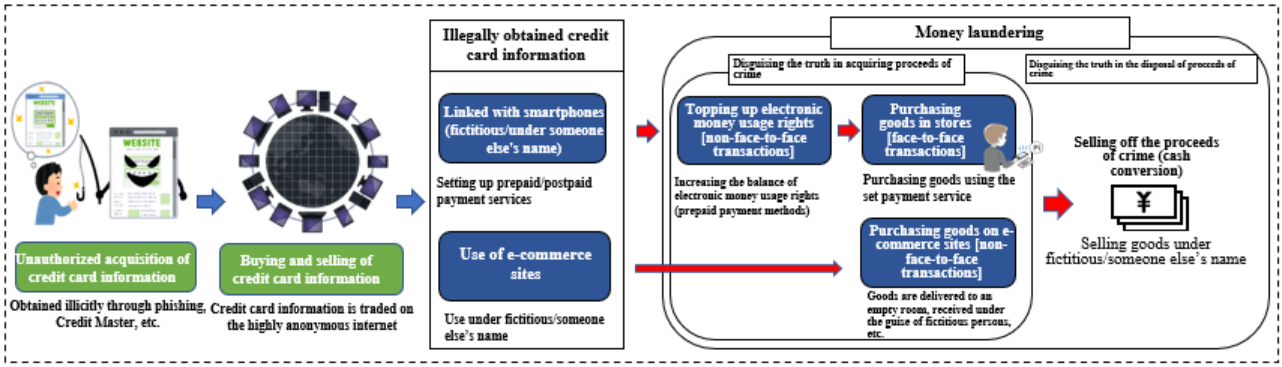
The following cases are common examples of misusing credit cards for money laundering:

- ○ A Boryokudan-related person accepted a credit card obtained through fraud from his friend free of charge and borrowed cash on the card for living costs and entertainment expenses.
- ○ 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 pretended to put goods up for sale on a shopping site and received payments for drugs by calling them as payments for the goods made with credit cards on the shopping site's payment system.
- ○ An offender used fraudulently obtained credit card information to impersonate the cardholder and rent a car from an internet site, thereby avoiding payment for its use.
- ○ 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.

---

*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).

Table 44: Image of Money Laundering Misused by Credit Cards



(ii) Trends of STRs

The number of STRs submitted by credit card operators was 105,148 between 2020 and 2022.

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 45: 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	31,281	29.7
3. Transactions under fictitious or other party's name	23,664	22.5
13. Customers with unusual behavior or movements	13,375	12.7
12. Transactions related to Boryokudan gangsters or their related parties	12,072	11.5

(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. The main relevant laws and regulations are as follows:

○ 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, etc. for industry associations and specified business operators.

[**Guidelines, etc. Established by Competent Authorities**]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism in Credit Card Business	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 in 2022]
<Ministry of Economy, Trade and Industry>
- Provided specified business operators with training, etc. 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 Countering the Financing of Terrorism in the Credit Card Business, 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 measures, including those against money laundering.

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, renewal, etc., 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 in 2022]
- Provided information, including information on ML, at an information meeting for members in 9 areas in Japan. (Japan Consumer Credit Association).
- Conducted video distribution to members on the responses by credit card companies based on the Revised Guidelines on Anti-Money Laundering and Counter-Terrorist Financing in the Credit Card Industry (Japan Consumer Credit Association).

(iv) 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.

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, and credit card operators taking ineffective 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.

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, customer attributes, etc.:

- ○ 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

[Status of Consideration for Strengthening Security Measures in Credit Card Payment Systems]

With the spread of e-commerce and cashless payments, the credit card payment market has been continuously expanding. However, against the backdrop of increasing cyber-attacks, the amount of damage from fraudulent use of credit cards has been rising, reaching a record high of approximately 43.67 billion yen[*1] in 2022.

As the government aims to expand cashless payments, the security risks, such as cyber-attacks, are increasing yearly, and the actual amount of damage from fraudulent use is also rising. In light of this situation, the country has launched the Study Group on Strengthening Security Measures in Credit Card Payment Systems to promote the implementation of additional measures in addition to the efforts by the industry.

The study group (from August 2022 through January 2023) conducted more detailed considerations, including technical aspects, in line with three directions:

1) Secure management of credit card numbers (preventing leakage)
2) Preventing fraudulent use of credit card numbers (preventing unauthorized use)
3) Raising awareness about the safe and secure use of credit and deterring crimes

The *Report on the Study Group on Strengthening Security Measures in Credit Card Payment Systems* (January 20, 2023), compiled based on the discussions in the study group, discusses the current situation of credit card fraud, future challenges, etc.

- ○ It states that credit cards, with the diversification of payment functions, tend to involve a variety of players in the credit card payment network.
- ○ In 2021, theft of credit card numbers and similar data accounted for 94% of all credit card fraud, with the primary cause being the fraudulent use of credit card numbers in non-face-to-face transactions.
- ○ The credit card numbers targeted for fraudulent use are assumed to be obtained not only from leaks by businesses in the credit card payment network, including e-commerce merchants, but also through credit master schemes exploiting the credit card payment processing of e-commerce merchants to figure out credit card numbers, and phishing that tricks users into giving away their credit card numbers via emails and text messages.
- ○ With the increase in e-commerce sites and the expansion of credit card payment use on these sites, the differences in transaction mechanisms between face-to-face and non-face-to-face credit card payments have become more pronounced.
- ○ Most transactions targeted for fraudulent use are non-face-to-face, involving easily resalable goods with cash value or goods that do not requires delivery. However, recently, the range of goods targeted for fraudulent use has diversified depending on the demand for goods at the time, and there has been an increase in fraudulent use of relatively low-priced goods.
- ○ It is essential to implement identity verification for users in non-face-to-face transactions, including gradually introducing mechanisms that use information only the user would know or possess, such as one-time passwords, other than fixed passwords, as proper verification of users.
- ○ Bearing the actual loss of credit card fraud by businesses so that users do not suffer economic damage is not enough. The goal is to prevent the occurrence of fraudulent use. It is essential to raise the level of security measures of all players to prevent the flow of funds into social crimes through the credit card payment system and, thereby, contribute to counter-terrorist financing measures.
- ○ Preventing the unauthorized use of credit card numbers and similar data is vital not only to ensure the reliability of the credit card payment system from property damage caused by impersonation using leaked or discovered credit card numbers but also to deter the flow of funds into social crimes through the credit card payment system, ultimately contributing to counter-terrorist financing measures.

*1 The *Compilation of Results on Credit Card Fraud* by the Japan Credit Association (June 30, 2023)

(12) Real Estate Dealt with by Real Estate Brokers

(i) Factors that Increase Risks

(A) Characteristics

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, usage of the property, etc., 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.

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 129,064 brokers as of the end of March 2023. In 2021, the annual amount of sales was about 49 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 2022, was about 170,000. 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 money laundering:

- ○ The proceeds derived from prostitution were used to purchase land in a relative's name.
- ○ A drug trafficker, etc., purchased real estate for living or for the manufacture of drugs in the name of a friend by using proceeds obtained from the illicit sale of drugs (a case in a foreign country)

(ii) Trends of STRs

The number of STRs submitted by real estate brokers was 22 between 2020 and 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 46: Reporting Status of Major STRs by Real Estate Brokers

Reason for report	Number of reports	Percentage (%)
1. Large cash transactions	13	59.1
20. Customers with unusual behavior or movements	3	13.6

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.

- ○ STR of transactions where a large amount of cash was paid, which was not appropriate for the customers' ages, occupations, etc.
- ○ STR about a suspicious source of funds, such as a customer who tends to stick with cash transactions as their payment method.
- ○ STR about transactions of customers who may have been involved in fraud as a result of searching public information.

○ STR, where beneficial owners of legal persons were found to be Boryokudan gangsters as a result of the investigation.

(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. The main relevant laws and regulations are as follows:

○ Real Estate Brokerage Act

Stipulates that the competent authorities have the right to collect reports from, conduct on-site inspection at, and give guidance, etc. 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, etc., 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

In order to promote AML/CFT, specified business operators must implement the required measures appropriately. In order to ensure this, the competent regulatory authorities are developing and updating supervisory guidelines, formulating the Guidelines on Anti-Money Laundering and Counter-Terrorist Financing Measures in Real Estate Transactions, and strengthening risk-based inspection and supervision to check whether businesses are implementing CDD measures in accordance with these guidelines. Various initiatives, including lectures and training for industry associations and specified business operators, are being advanced.

[Guidelines, etc. Established by the Competent Administrative Authority]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines on Anti-Money Laundering and Counter-Terrorist Financing Measures 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 in 2022]
<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.

(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 in 2022]
- Informed member companies about the results of the FATF's mutual evaluation of Japan and the promotion of further ML/TF countermeasures through the dissemination of *the Guidelines on Anti-Money Laundering and Counter-Terrorist Financing Measures in Real Estate Transactions* (Liaison Council for Preventing Transfer of Criminal Proceeds and Damage Caused by Anti-social Forces in Real Estate Business).

(iv) 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.

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 on Anti-Money Laundering and Counter-Terrorist Financing Measures in Real Estate Transactions 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.

Considering the cases where real estate brokers were misused for money laundering, etc., 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, customer attributes, etc.

(13) Precious Metals and Stones Dealt with by Dealers in Precious Metals and Stones

(i) Factors that Increase Risks

(A) Characteristics

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.

The FEFTA requires any person who exports or imports precious metals[*1] of more than 1 kg by carrying them to notify 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 2021 administrative year,[*2] the number of processed cases (notifications and indictments) of gold smuggling was 13 (35% decrease compared to the previous administrative year), and the value of evaded taxes was about 20 million yen (77% decrease 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 has been decreasing. 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. Smuggling routes have diversified for example air passengers, and air freight, international mail are used for the routes. When looking in terms of the source of smuggling, Hong Kong, Korea, China, 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.

---

*1 Means precious metals set forth in Article 6, paragraph 1, item 10 of the FEFTA.
*2 The period from July 2021 to June 2022.

(B) Typologies

The following cases are common examples of misusing precious metals and stones for money laundering:

○ An offender forced an acquaintance to sell gold bullion obtained through theft to a gold dealer in the name of a legal person.

○ Precious metals were purchased under fictitious or other party at a jewelry store using cash obtained through theft.

○ 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 money laundering due to their high anonymity and ease of liquidation and transportation.

(ii) Trends of STRs

The number of STRs submitted by dealers in precious metals and stones was 235 between 2020 and 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 47: Reporting Status of Major STRs by Dealers in Precious Metals and Stones

Reason for report	Number of reports	Percentage (%)
17. Frequent in a short-term, multiple transactions	47	20.0
1. Large cash transactions	42	17.9
3. Economically unreasonable transactions	34	14.5

(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. The main relevant laws and regulations are as follows:

○ Secondhand Goods Business Act

Stipulates that police officers have the right to conduct on-site inspections, etc. 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, etc., 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.

[**Guidelines, etc. Established by Competent Authorities**]

Name of Guidelines, etc.	Website's URL, etc.
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 in 2022]
<Ministry of Economy, Trade and Industry>
- 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. (June 2022)

(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 business operators understand AML/CFT measures by preparing and distributing leaflets that describe the overview of the Act on Prevention of Transfer of Criminal Proceeds and the details of their obligations, holding seminars on AML/CFT measures, and updating the website designated for AML/CFT measures.

The Japan Reuse Affairs Association and Antique Dealers Federation of Tokyo are informing their members etc. on AML/CFT by reminding their members of the obligations associated with precious-metal transactions under the Act on Prevention of Transfer of Criminal Proceeds, etc., 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.

[Examples of Initiatives Taken by Industry Associations in 2022]
- Held training sessions for member companies to explain the Guidelines on Anti-Money Laundering and Counter-Terrorist Financing Measures in Dealers in Precious Metals and Stones, among others, implementing thorough awareness of ML/TF measures. (Japan Gold Metal Association)
- Distributed awareness materials created by the Ministry of Economy, Trade and Industry via email to association members, published them in the association's magazine and on its website, and also distributed them at jewelry exhibition venues, implementing thorough awareness. (Japan Jewelry Association)

(iv) 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.

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 Dealers 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.

Considering the cases where dealers in precious metals and stones were misused for money laundering, 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, customer attributes, etc.:

- Transactions under anonymous or fictitious, borrowed names, 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, assets, etc.

(14) Postal Receiving Services Dealt with by Postal Receiving Service Providers

(i) Factors that Increase Risks

(A) Characteristics

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 fraud etc., in online and telephone fraud, etc.

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 2020 and 2022. Specific violations identified through the submitted reports are as follows:

- ○ Failed to verify identity and other information at the time of transactions by reviewing identification documents presented by customers as specified in the rules.
- ○ 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 rules.

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 money laundering:

- ○ 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 fictious or other party's name.

(ii) Trends of STRs

The number of STRs from postal receiving service providers between 2020 and 2022 was 3.

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, etc., 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 48: Reporting Status of Major STRs by Postal receiving Services

Reason for report	Number of reports	Percentage (%)
6. Transactions under fictitious or other party's name	1	33.3
9. Customers with unusual behavior or movements	1	33.3

(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 at the time of transactions, and also stipulates that the competent authorities have the right to require reports or submission of documents, conduct on-site inspections, and take other action to supervise specified business operators.

(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 developing and updating supervisory guidelines, formulating the Guidelines on Anti-Money Laundering and Counter-Terrorist Financing Measures in Postal receiving Services, and strengthening risk-based inspection and supervision to check whether businesses are implementing CDD measures in accordance with these guidelines. Various initiatives, including lectures and training for industry associations and specified business operators, are being advanced.

[Guidelines, etc. Established by Competent Authorities]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism in Postal Receiving Services	https://www.meti.go.jp/policy/commercial_mail_receiving/pdf/20211224yuubinbutumanerongl.pdf(Ministry of Economy, Trade and Industry)

[Examples of Initiatives Taken by Competent Authority in 2022]
<Ministry of Economy, Trade and Industry>
- Conducted an explanatory meeting for businesses about the Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism in Postal Receiving Services, formulated and announced in December 2021 (March 2022).
- Based on the results of surveys conducted with businesses, carried out risk assessments for each company and performed inspections and guidance based on the Act on Prevention of Transfer of Criminal Proceeds for 2 companies, considering the risk evaluation (December 2022).

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 conducted reports and specific guidance based on the Act on Prevention of Transfer of Criminal Proceeds to the concerned businesses. In 2022, a correction order was issued to 1 postal receiving service provider recognized for violating the obligation of verification at the time of the transaction, including measures to ensure compliance with the obligations for verification and recording at the time of transactions and the development of measures to prevent a recurrence.

(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) 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.

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 Countering 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.

Furthermore, considering the cases where postal receiving services were misused for money laundering, 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, customer attributes, etc.:

- ○ Transactions under anonymous or fictitious, borrowed names, 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

(15) Telephone Receiving Services Dealt with by Telephone Receiving Service Providers

(i) Factors that Increase Risks

(A) Characteristics

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, etc.

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 money laundering 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 a money laundering 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 2020 and 2022 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, and also stipulates that the competent authorities have the right to require reports or submission of documents, conduct on-site inspections, and take other action to supervise specified business operators.

(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 developing and updating supervisory guidelines, formulating *the Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism in Telephone Receiving Services and Telephone Forwarding Services*, and strengthening risk-based inspection and supervision to check whether businesses are implementing CDD measures in accordance with these guidelines. Various initiatives, including lectures and training for industry associations and specified business operators, are being advanced.

[Guidelines, etc. Established by Competent Authorities]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism in Telephone Receiving Services and Telephone Forwarding Services	https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/money/top.html (Ministry of Internal Affairs and Communications)

[Examples of Initiatives Taken by Competent Authorities in 2022]
<Ministry of Internal Affairs and Communications>

- Posted documents on the website of the Ministry of Internal Affairs and Communications explaining the measures that telephone receiving service providers and telephone forwarding service providers are required to take under the Act on Prevention of Transfer of Criminal Proceeds.
- Conducted a written survey to grasp the status of compliance with laws and regulations as well as risk management by telephone-receiving service providers and telephone-forwarding service providers. (March 2022)
- 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 2022)

(iv) Assessment of Risks

Recently, we have not seen any cleared cases for money laundering 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 Countering 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) Characteristics

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 2023, 920 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. 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[*2] 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 21 reports in accordance with the Act on Prevention of Transfer of Criminal Proceeds during the period from 2020 to 2022. The details of major violations of obligations discovered as a result of collecting the reports in 2022 are as follows:

- ○ Failed to verify identity and other information at the time of transactions by reviewing identification documents presented by customers as specified in the rules.
- ○ 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 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 money laundering:

- ○ In a case of concealing criminal proceeds derived from the sale of obscene DVDs, multiple telephone-

---

*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.

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

There were 4 STRs from telephone forwarding service providers between 2020 and 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 49: 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	25.0
5. Transactions under fictitious or other party's name	1	25.0
8. Customers with unusual behavior or movements	1	25.0

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. The main relevant laws and regulations are as follows:

○ 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 developing and updating supervisory guidelines, formulating the Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism in Telephone Receiving Services and Telephone Forwarding Services, and strengthening risk-based inspection and supervision to check whether businesses are implementing CDD measures in accordance with these guidelines. Various initiatives, including lectures and training for industry associations and specified business operators, are being advanced.

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 etc. Established by Competent Authorities]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism in Telephone Receiving Services and Telephone Forwarding Services	https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/money/top.html (Ministry of Internal Affairs and Communications)

[Examples of Initiatives Taken by Competent Authorities in 2022]
<Ministry of Internal Affairs and Communications>
- Posted documents on the website of the Ministry of Internal Affairs and Communications explaining the measures that telephone receiving service providers and telephone forwarding service providers are required to take under the Act on Prevention of Transfer of Criminal Proceeds.
- Conducted a written survey to grasp the status of compliance with laws and regulations as well as risk management by telephone receiving service providers and telephone forwarding service providers. (March 2022)
- 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 2022)

Based on the statement of opinion derived from the results of the abovementioned submission reports collected by the National Public Safety Commission, the Ministry of Internal Affairs and Communications collects reports, etc., from the operators in question under the Act on Prevention of Transfer of Crime Proceeds and to provide individual and specific guidance, etc. In 2022, the Ministry issued a rectification order to 3 telephone forwarding service providers that were recognized to have violated the obligation to conduct verifications at the time of transactions, requiring the providers to fully understand and comply with the laws related to performing verifications at the time of transactions and the preparation of verification records, and to implement measures, etc. to prevent a recurrence.

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, occupations of customers, etc.
○ 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 consider the necessity for reporting 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, etc., 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, etc., 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 in 2022]
- From December 2022, the Japan Unified Communications Carriers Association (JUSA), 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, etc. (JUSA).
- JUSA has implemented 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. Moreover, JUSA actively works towards risk reduction by exchanging information with related government agencies, providing members with the latest information, and issuing warnings.

(iv) 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.

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 Countering 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.

In addition, considering the cases where telephone forwarding services were misused for online and telephone fraud, etc., 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.

(17) Legal/Accounting Services Dealt with by Legal/Accounting Professionals[*1]

(i) Factors that Increase Risks

(A) Characteristics

There are lawyers, judicial scriveners, and administrative scriveners who possess legal expertise as professionals, as well as certified public accountants and certified public tax accountants who possess accounting expertise as professionals.

Lawyers provide legal services at the request of a client or other person concerned. A lawyer 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 2023, 44,916 lawyers, 4 Okinawa special members, 455 foreign lawyers, 1,598 legal profession corporations, and 8 foreign legal profession corporations are registered in Japan.

Judicial scriveners provide services related to registration on behalf of clients, consult about registration, and engage in business related to legal representation in summary court, etc. A judicial scrivener 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 2023, 23,059 judicial scriveners and 1,106 judicial scrivener corporations are registered.

Administrative scriveners 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, administrative scriveners can carry out procedures as agents to submit documents to public offices. Administrative scriveners 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 2023, 51,041 administrative scriveners and 1,196 administrative scrivener corporations are registered.

Certified public accountants shall make it their practice to audit or attest to financial statements. They may also make it their practice to compile financial statements, to examine or plan financial matters, or to be consulted on financial matters, using the title of certified public accountant. A certified public accountant 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 2023, 34,445 certified public accountants, 2 foreign certified public accountants, and 279 audit firms are registered.

Certified public tax accountants represent clients in filing applications and requests, reporting, preparing statements under laws regarding tax payments to tax agencies, preparing tax forms, and consulting about taxation. Other than that, as the incidental business of the mentioned above, they prepare financial forms, keep accounting books on behalf of their clients, and provide a range of services related to finance. A certified public tax accountant must be registered on the roll of certified public tax accountants kept by the Japan Federation of Certified Public Tax Accountants' Associations (hereinafter referred to as "JFCPTAA"). As of the end of March 2023, there were 80,692 certified public tax accountants and 4,844 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.

[*1] Legal/accounting professionals mean those listed in Article 2, paragraph 2, item 45 (lawyer or legal professional corporation), item 46 (judicial scrivener or judicial scrivener corporation), item 47 (administrative scriveners or administrative scrivener corporation), item 48 (certified public accountant or administrative scrivener corporation), and item 49 (certified public tax accountant or certified public tax accountant corporation) of the Act on Prevention of Transfer of Criminal Proceeds.

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.

(B) Typologies

The following cases are common examples of misusing legal/accounting services for money laundering:

- ○ 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, etc., 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 verify identification data 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) 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.

Pursuant to the provisions of the Act on Prevention of Transfer of Criminal Proceeds, the JFBA sets rules and regulations that stipulate the duties of lawyers. These include the verification of client identity 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. Furthermore, the JFBA requires individual lawyers to submit an annual report in regard to

verification of client identity, retention of records, and any other AML/CFT obligation under the JFBA's rule[*1].

(B) Measures by competent authorities and self-regulated organizations

Competent authorities and associations of each 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 regulations, 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) and the explicit consideration of the Risk Assessment for Money Laundering in Legal Practice (hereinafter referred to as "Legal Practice Risk Assessment for ML"), following the amendment to the Act on Prevention of Transfer of Criminal Proceeds in December 2022. Furthermore, in order to encourage lawyers 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, and compiled the results into the Legal Practice Risk Assessment for ML. The report was posted in the JFBA's journal *Liberty and Justice* that is distributed to all members, as well as on the JFBA's website. In addition, the JFBA prepared tools, FAQs, and online courses to promote compliance with the JFBA's regulations, etc. concerning AML/CFT by lawyers and provided them to lawyers 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, etc. in its journal *Liberty and Justice* to inform its members of AML/CFT and share information.

In light of the actual situation identified by the JFBA, lawyers 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 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. Japan Federation of Shiho-Shoshi's Associations (JFSA)

JFSA promotes judicial scriveners 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

---

* [1] The amendment to the Act on Prevention of Transfer of Criminal Proceeds, enacted in December 2022 following the FATF Recommendations Compliance Act, stipulates that, except for matters related to confidentiality obligations, certified administrative procedures legal specialists, certified public accountants, and certified public tax accountants are required to submit STRs. This amendment is to be enforced from a date specified by a Cabinet Order within a period not exceeding one year and six months from the date of promulgation. Furthermore, obligations have been added for certified administrative procedures legal specialists, certified public accountants, certified public tax accountants, and judicial scriveners to verify the purpose of transactions, the nature of their occupation or business, and, in the case of corporations, their ultimate beneficial owners besides the identity of clients. This includes verifying the assets and income status in high-risk transactions for certified administrative procedures legal specialists, certified public accountants, and certified public tax accountants.
Additionally, for lawyers, measures equivalent to transaction time verification are planned to be established in the rules of the JFBA

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.

In light of the actual situation identified by the competent authorities, judicial scriveners 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. 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.

c. Japan Federation of Certified Administrative Procedures Legal Specialists Associations (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 administrative scrivener members since January 2018 to ensure that all members properly conduct identity verifications and prepare transaction records, etc. 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 administrative scriveners, in light of the survey results on the actual status of services of administrative scriveners 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.

In addition, in response to the amendment of the Act on Prevention of Transfer of Criminal Proceeds in December 2022, we are considering revising the *Identity Verification Handbook based on the Act on Prevention of Transfer of Criminal Proceeds* published for certified administrative procedures legal specialists.

In light of the actual situation identified by the competent authorities, administrative scriveners 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 administrative scriveners.

d. Japanese Institute of Certified Public Accountants (JICPA)

JICPA conducts an annual survey of certified public accountants and audit firms on their status of compliance with the Act on Prevention of Transfer of Criminal Proceeds.

Furthermore, the website for JICPA members introduces e-learning training and publications related to ML/TF published by FATF. The JICPA also held seminars taught by external specialists for its members on the overview of the Act on the Prevention of Transfer of Criminal Proceeds and the need for AML/CFT measures. 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 should pay attention to the following matters for AML/CFT measures:

○ There are restrictions on specified services that certified public accountants and audit firms can perform due to business restrictions under the provisions of the Certified Public Accountant Act 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.

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 on their status of compliance with the Act on Prevention of Transfer of Criminal Proceeds. In collaboration with the National Tax Agency, JFCPTAA 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, and by distributing via the Internet and DVD training videos, and by revising the guidelines on the internal control systems, etc. for certified tax accountant offices.

In light of the actual situation identified by the competent authorities, certified public tax accountants and their corporations 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 have made improvements and corrections with respect to these matters by providing instructions, etc., to certified public tax accountants and certified public tax accountants' corporations.

(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 the 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, etc.

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, etc., 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.

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.

Considering the cases where legal/accounting professionals were misused for money laundering, 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, customer attributes, etc.

[High-Value Electronically Transferable Prepaid Payment Instruments Dealt with by Issuers]

1. Factors that Increase Risks

(1) Characteristics

Prepaid payment instruments under the Payment Services Act 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 regulatory authority, and issuers of prepaid payment instruments for third-party business must register with the regulatory authority.

Furthermore, among prepaid payment instruments for third party business, those capable of electronic value transfer and allowing high-value charges and transfers were defined 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 will be added as specified business operators under the Act on Prevention of Transfer of Criminal Proceeds.

Generally, under the Payment Services Act, refunds of unused balances purchased (charged) are prohibited, except in cases of the issuer's closure, preventing users from freely withdrawing cash equivalent to the charged 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.

(2) Cases

The main cases of misuse of prepaid payment instruments for money laundering are as follows:

- ○ Selling electronic money rights (prepaid payment instruments) obtained through fraud via internet brokers and depositing the sales proceeds into an account under a fictitious name or the name of other individual.
- ○ Using fraudulently obtained credit card information, electronic money rights (prepaid payment instruments) were charged to a virtual prepaid card created online under a fictitious name or the name of other party, which was then used for payment of living expenses, among other things, or 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, etc., using electronically obtained electronic money rights (prepaid payment instruments) of other party, impersonating the holder.

2. Measures to Mitigate Risks

(1) Statutory measures

In order to implement AML/CFT, each relevant law and regulation contains on measures to mitigate risks. The main relevant laws and regulations are as follows:

- ○ Act on Prevention of Transfer of Criminal Proceeds

  In June 2022, the Act on Prevention of Transfer of Criminal Proceeds was amended to newly include issuers of high-value electronically transferable prepaid payment instruments as specified business operators, mandating transaction verification, preparation and preservation of verification records, transaction records, and obligations to submit STRs.
- ○ Payment Services Act

  Considering user protection, specifications are set for product features, system-related issues, monitoring methods, and policies for dealing with misuse towards users.

  Also, in June 2022, the Payment Services Act was amended to impose the obligation to submit a business implementation plan on issuers of high-value electronically transferable prepaid payment instruments to strengthen monitoring by the administrative authority.

(2) Measures by competent authorities

Efforts such as awareness-raising are being advanced not only from the perspective of preventing money laundering offences but also from preventing overall crime victimization by related ministries, industry associations, etc.

- ○ 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).

---

*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 charged 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.

○ 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).

3. Risk Level

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 charged. Currently, many issuers set a maximum charge limit and restrict the use of charged 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 process of money laundering, 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 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 charges and transfers is limited, services allowing charges 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.

[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 money laundering 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 money laundering 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
The FATF Recommendations also 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.
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 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 amended by the Order for Enforcement of the IR 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, etc., of chips (transactions of issuing, granting, or receiving chips) in which the value of the chips exceeds 300,000 yen
○ Receiving money pertaining to specified fund receipt services
○ Transactions involving receipt or payment of casino-related money (refund of money pertaining to specified fund receipt services, receipt of payment of claims pertaining to a specified fund loan contract, or money exchange) in which the value of the transaction exceeds 300,000 yen
○ Provision of premiums related to casino gaming (so-called "complimentary") in which the value of the premiums 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 development laws and regulations require casino business operators for various obligations including the following initiatives in addition to the restrictions under the Act on Prevention of Transfer of Criminal Proceeds:
○ To prepare the Regulations on Prevention of Transfer of Criminal Proceeds (examined by the Casino Regulatory Commission)
○ 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 money laundering.
Subsequently, in April 2023, based on the IR 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.

*1 Vulnerabilities of Casinos and Gaming Sector (March 2009)

Section 6. Low-risk Transactions

According to the principles of a risk-based approach, when risks are high, strict measures to manage and mitigate the risks should be taken; on the other hand, when risks are low, simple measures can be taken. Therefore, transactions for which simple CDD is allowed are specified in Article 4 of the Ordinance.

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 Reduce Risks	Why the Factors in the Left Column are Considered to Reduce 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 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[*2].

---

*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 provide that when specified business operators conduct two or more transactions (receipt or payment of cash, withdrawal of deposit/savings, foreign currency exchange, sales of precious metal, etc.) with the same customer at the same time or continuously, and the transactions obviously represent a divided single transaction, the separate transactions should be regarded as a single transaction.

*2 In the Act on Prevention of Transfer of Criminal Proceeds and the Enforcement Order, transactions for which simplified CDD is permitted as prescribed by the Ordinance 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 permitted.

	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 1 of the Ordinance (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 2 of the Ordinance ((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 3, (a) of the Ordinance, 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,*1 etc., as set forth in Article 4, paragraph 1, item 3, (b) of the Ordinance	(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.*2 as set forth in Article 4, paragraph 1, item 4 of the Ordinance	(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 5 of the Ordinance	(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 6, (a) of the Ordinance	(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 6, (b) of the Ordinance	(i), (iii), (iv), (vi)
		Individual Credit*3,etc. set forth in Article 4, paragraph 1, item 6, (c) of the Ordinance	(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 7, (a) of the Ordinance	(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 7, (b) of the Ordinance	(viii)
		Payment of charges for electricity, gas, or water as set forth in Article 4, paragraph 1, item 7, (c) of the Ordinance	(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 7, (d) of the Ordinance	(viii)
		Exchange transactions of not more than 2 million yen for depositing and withdrawing funds as set forth in Article 4, paragraph 1, item 7, (e) of the Ordinance	(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	(vii), (viii)

*1 In group insurance, the amount that is deducted from the salary of employees is used for premiums.

*2 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.

*3 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.

		operators as set forth in Article 4, paragraph 1, item 7, (f) of the Ordinance	
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 8 of the Ordinance	(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 9 of the Ordinance*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 10 of the Ordinance	(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 11 of the Ordinance	(viii)
12	Certain Transactions with Telephone Receiving Services	Certain transactions with telephone receiving services as set forth in Article 4, paragraph 1, item 12 of the Ordinance ((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 13 (a) of the Ordinance	(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 13 (b) of the Ordinance	(i), (iii), (iv), (viii)
		Transactions conducted by a specified business operator with its subsidiary, etc., as a customer as set forth in Article 4, paragraph 1, item 13 (c) of the Ordinance	(i), (viii)
14	Specific Transactions in Agent Work, etc., for Specified Mandated Acts by Judicial Scriveners, etc.*3	Conclusion of contracts for voluntarily appointed guardians as set forth in Article 4, paragraph 3, item 1 of the Ordinance	(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 2 of the Ordinance	(i), (iv), (viii) and (ii) or (iii)

*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 9 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.

*3 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 46 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.

Going Forward

As a result of the FATF Fourth Round of Mutual Evaluation of Japan published in August 2021, the Government of Japan established the "Inter-Ministerial Council for AML/CFT/CPF Policy" (hereinafter referred to as the "Inter-Ministerial Council") jointly chaired by the National Police Agency and the Ministry of Finance in the same month. This was done to promote 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. This action plan aims to improve the legislative framework and the implementation of AML/CFT/CPF measures. Specifically, the action plan lists the following action items: renewing the National Risk Assessment, strengthening supervision of financial institutions, enhancing the transparency of beneficial ownership information, establishing a task force to improve the prosecution rate for money laundering offences, enhancing ML investigation and prosecution and increasing the prosecution rate of ML cases with the efforts including establishment of the task force, and prevention from abusing the nonprofit organization (NPO) sector.

In May 2022, the Inter-Ministerial Council established the "Basic Policy for Promoting AML/CFT/CPF Efforts" in order to examine the risks surrounding Japan and purposes of AML/CFT/CPF measures of Japan, further enhance collaboration between the relevant ministries and agencies, and improve the effectiveness of the measures.

In light of the fact that the factors that should be considered, such as the contents of the 2021 NRA-FUR, the spread of new technology, and the advancement of global discussions, have been enhanced and diversified, the Basic Policy for Promoting AML/CFT/CPF Efforts listed the following main points to take more realistic measures:

(i) Ensuring that a risk-based approach to AML/CFT/CPF is implemented;
(ii) Promptly adapting to new technology;
(iii) Enhancing international cooperation and collaboration; and
(iv) Enhancing collaboration between the relevant ministries and agencies as well as between the public and private sectors.

The formulated action plan is progressing smoothly, but in the future, under the policy conference, it is necessary to take into account changes in domestic and international situations, and with an eye on the Fifth Round of Mutual Evaluation of Japan by the FATF, to further strengthen the coordination among relevant ministries and agencies, and to enhance measures with a sense of urgency.

On their part, specified business operators will not only need to comply with the obligations under laws and regulations but also act to mitigate ML/TF risks through a risk-based approach. This will involve being aware of and identifying the characteristics of their operations and risks associated with them and further reviewing those risks.

For its part, the Government of Japan will need to implement AML/CFT/CPF measures in collaboration via public-private partnerships, and conduct proactive public relations activities that help the public to understand what the measures are so as to improve their effectiveness. The situation around Japan is changing minute by minute as new technology develops and through constant changes in AML/CFT/CPF initiatives that the international community expects. Meeting these changes and requests from the international community, as well as securing the safety and peace of the daily lives of the general public and helping to develop sound economic activities, requires everyone involved to fully grasp the ML/TF risks based on the contents of this NRA-FUR and act accordingly.