December 2022

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 Asset-Freezing Act	Act on Special Measures Concerning Asset Freezing, etc. of International Terrorists 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)
Firearms and Swords Control Act	Act for Controlling the Possession of Firearms or Swords and Other Such Weapons (Act No. 6 of 1958)
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)
Immigration Control Act Enforcement Ordinance	Ordinance for Enforcement of the Immigration Control and Refugee Recognition Act (Ordinance of the Ministry of Justice No. 54 of 1981)
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 Law	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)
Worker Dispatching Act	Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers (Act No. 88 of 1985)

Introduction

1. History

In modern society where information technology and globalization of economic/financial services are advancing, the state of money laundering 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 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 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[*1] 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[*2], etc. in keeping with the contents of the NRA-Baseline Analysis.[*3]

2. Purpose

The FATF Recommendations (Recommendation 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 approach (e.g., applying enhanced CDD to higher risk transactions). As a prerequisite, 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.

In order to carry out verification at the time of transactions, etc. accurately, the Act on Prevention of Transfer of Criminal Proceeds and Ordinance 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

---

*1 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.

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

*3 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.

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, the risks surrounding Japan are indicated from the viewpoints of geographical environment, social environment, economic environment, criminal circumstances, and so on. In Section 3, the offenders of ML/TF (such as Boryokudan, fraud (phone scam) groups, and crime groups of foreigners in Japan)[*1], major predicate offenses (such as thefts, frauds, and drug-related crimes), and transactions misused for ML/TF (such as domestic exchange transactions and cash transactions) are analyzed.

In Section 4, non-face-to-face transactions, cash transactions, and international transactions are assessed as high-risk transactions from the viewpoint of transaction type, as well as transactions related to Iran and North Korea from the viewpoint of countries and regions, and transactions with international terrorists and legal persons without transparency of beneficial owner, etc. from the viewpoint of customer attributes.

In Section 5, products and services handled by deposit-taking institutions, funds-transfer service providers, and crypto-assets exchange service providers, which are specified business operators, are assessed as being at a relatively higher risk than those handled by specified business operators in other forms of business.

*1 Foreigners in Japan refers to foreigners residing in Japan, except so-called long-term residents (permanent residents, their spouses, etc. and special permanent residents), U.S. forces in Japan, and persons with unknown visa status.

[Overview of NRA-FUR]

➢ **General Risk Assessment** ➢ **Individual Risk Assessment**

Environments Surrounding Japan (pages 9 to 12)
1. Geographical environment 2. Social environment 3. Economic environment 4. Criminal circumstances

Analysis of Money Laundering Cases, etc.		
Offenders (pages 13-17)	**Modus Operandi (pages 18-27)**	**Suspicious Transaction Report (pages 28-32)**
1. Boryokudan 2. Fraud(phone scam) 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 reports submitted by each form of business

➢ **Risk Assessment (i) (High-risk transaction types, countries/regions, and customer attributes)**

Transaction Types (pages 33-43)	**Countries/Regions (pages 44-46)**	**Customer Attributes (pages 47-67)**
1. Non-face-to-face transactions 2. Cash transactions 3. International transactions (such as remittance to foreign countries funded with a large amount of cash)	1. Countries and regions against which the implementation of countermeasures is requested by the FATF Recommendations (particularly high-risk): Iran and North Korea 2. Countries and regions for which failures in measures have been pointed out in the FATF Recommendations (high-risk): None (Results of October 2021 FATF meeting)	1. Anti-social forces (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 owner, etc.)

➢ **Risk assessment (ii) (Products/services)**

	Products/Services (pages 68-144)		
Transactions of relatively higher risk than other business forms	● Products/services dealt with by deposit-taking institutions ● Fund transfer services ● Crypto-assets		
Transactions considered to be of risk	● Insurance ● Investment ● Trust ● Money lending ● Foreign currency exchanges	● Financial 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 (pages 145-149)	
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 and 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

Although the structure of this NRA-FUR does not differ significantly from the 2021 NRA-FUR, it has been updated and improved based on the changes in circumstances in Japan and abroad as well as the results of the Fourth Round of Mutual Evaluation of Japan, etc.

The main updates and improvements are as follows:

(1) This NRA-FUR has added descriptions on the status of use of STRs by investigative organizations other than the police, risk assessment by administrative agencies responsible for non-profit organizations (NPOs), as well as threats and vulnerabilities, etc. discovered by competent authorities based on information obtained from the law enforcement agencies (LEAs) and relevant ministries and agencies.

(2) It introduces trends in environmental crimes and crypto-assets around the world, which have drawn attention internationally, and circumstances surrounding Japan in reference to FATF reports, etc.

(3) It also organizes information on modus operandi and corporations that have been used for abusing cross-border transactions, and provides updated cases of money laundering to enrich knowledge about ML/TF risks in Japan.

This NRA-FUR introduces the guidelines, etc. prepared and published by the competent authorities, etc. to promote AML/CFT measures, and adds descriptions of initiatives taken by competent authorities, industry associations and specified business operators in connection with AML/CFT measures in 2021. Furthermore, information on so-called stablecoins and high-value, electronically transferrable prepaid payment instruments (defined in the Payment Services Act amended in 2022), etc. has been added in light of the amendment of the Act on Prevention of Transfer of Criminal Proceeds and other laws.

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. Example: Criminals, and terrorist groups, and their facilitators, and their funds, ML/TF activities, etc.
Vulnerability	Things that can be exploited by the threat 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), fraud (phone scam) groups, and crime groups of foreigners in Japan, and predicate offenses 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.

---

*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.

○ Consequence

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 groups 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 groups, 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 offenses, 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 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 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 criminal groups.

2. Social Environment

The total population of Japan as of October 1, 2021 was approximately 125,500,000, marking 11 consecutive years of decrease. The ratio of the population aged 65 and over to the total population reached a record high of 28.9%, which is higher than 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 100,000,000 in 2053.

The number of foreigners entering Japan in 2021 was approximately 350,000, 91.8% less than in the previous year. This is a significant decrease since February 2020, when the government's measures against the COVID-19 pandemic began. The total number of new arrivals is approximately 150,000. As far as the number of new arrivals by nationality and region is concerned, the number of Vietnamese was the largest, followed by Chinese 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 2021 was approximately 2,760,000, 4.4% less than the previous year. In terms of the number of foreign residents by nationality and region, Chinese was the largest and accounted for 26.0% 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 2021 (Quarterly Estimates of GDP for Apr.-Jun. 2022 (The Second Preliminary Estimates)) was 541.4 trillion yen, the third-largest economy after the United States and China. In terms of purchasing power parity GDP in 2021, it is the fourth largest globally after China, the United States, and India. The real GDP growth rate in FY2021 was 2.3%. The share of nominal gross value added by economic activity in 2020 was 1.0% for the primary industry, 25.9% for the secondary industry, and 73.1% for the tertiary industry. Regarding the trade value in 2021, Japan's exports amounted to 83,091.4 billion yen, and imports amounted to 84,875.0 billion yen. Japan's main export partners were China, the United States and Taiwan, etc., and its import partners were China, the United States and Australia, etc.

In Japan, cross-border transactions are conducted freely. However, economic sanctions based on international cooperation and economic sanctions based on Japan's own decision 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.

Besides, Japan has a highly developed financial sector as a global financial center. A considerable amount of financial transactions is 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 of 2021, the number of branch offices of major financial institutions[*1] was 37,532 (including 173 overseas branch offices). There were 91,000 ATMs[*2] installed with ease of access to the financial system. Furthermore, three of the 30 global systemically important banks (G-SIBs) designated by the Financial Stability Board (FSB) in 2021 were Japanese megabanks.

In terms of the scale of financial transactions in Japan, the balance of bank deposits at the end of March 2022 was approximately 1,117 trillion yen. As for settlement transactions in 2021, domestic exchange transactions (other banks' transaction volume of exchange) comprised approximately 3,062 trillion yen (approximately 1.7 billion cases), with a daily average of about 12 trillion yen (approximately 7.11 million cases), and the amount of foreign exchange in settled in yen was approximately 4,474 trillion yen (approximately 6.83 million cases), with a daily average of about 18 trillion yen (approximately 27,000 cases).

Next, regarding the securities market size, Japanese stock market capitalization was approximately 753 trillion yen as of the end of December 2021. The trading value of listed stocks held on the Tokyo Stock Exchange (1st Section and 2nd Section) in 2021 was approximately 774 trillion yen.

---

*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 bank ATMs was calculated as of the end of September 2021, and the number of Japan Post Bank ATMs was calculated as of the end of March 2021.

As for cash transactions, since the number of financial institution branches and ATMs is large, withdrawing cash from deposit accounts and depositing money into accounts is convenient. Furthermore, there is a high level of anti-counterfeiting technology for banknotes and few counterfeit bills in circulation. Due to the above facts, the cash distribution situation in Japan is higher than in other countries. However, cash transactions have decreased relatively, with the rise in the cashless payment ratio[*1] due to the progress of cashless payments. The above situation is expected to lead to restraint of ML/TF related to cash transactions.

On the other hand, 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

Among the indicators for measuring Japan's criminal circumstances, the total number of recognized criminal offense cases was 568,104 (7.5% decrease compared to the previous year), which continues to be a record low after the war as in the previous year. In addition, the rate of decrease from 2002, when the number of recognized criminal offense cases was the highest after the Second World War, was 80.1%. The total number of cleared cases of criminal offences was 264,485, a 5.3% decrease compared to the previous year; however, the percentage of cleared cases was 46.6%, up 1.1 point from the previous year. The percentage of elderly victims among the total number of victims in the cases of recognized criminal offences has consistently risen. In 2021, it was 12.3%, up 3.1 points compared to 10 years ago (2011). In terms of the type of crime, the rate of damage to the elderly is increasing for all crime types. In particular, the increase in intelligence crimes, such as fraud, is remarkable, and it was 32.0% in 2021, an increase of 13.4 points from 2011. Furthermore, in terms of crimes by fraud (phone scam) groups, which affect many elderly people, the percentage of elderly victims among the total number of victims in recognized cases of fraud (phone scam) (excluding corporate victims) was 88.2% in 2021.

Next, looking at the number of cleared cases of cybercrime[*2], which has been increasing in recent years, the number was the highest ever in 2021 (12,209 cases) (see Table 1).

Table 1 [Status of Cybercrime Cleared Cases]

	2017	2018	2019	2020	2021
Number of cleared cases	9,014	9,040	9,519	9,875	12,209

It is thought that in many of the online banking fraud cases, short message services (SMS) and emails were used to lead victims to phishing sites disguised as financial institutions or courier companies. Both the number of online banking fraud cases (584 cases, a 66.3% decrease from the previous year) and the amount of loss from online banking fraud (approximately 820,000,000 yen, a 27.6% decline from the previous year) in 2021 fell compared to the previous year. On the other hand, according to the Council of Anti-Phishing Japan, the number of reports on phishing attacks in 2021 was 530,000 cases, and this figure has been steadily increasing [*3] (see Table 2). According to the results of analysis[*4] by the Japan Cybercrime Control Center (JC3), not many of the phishing sites detected in 2021 were disguised as a bank. Instead, many sites were disguised as an e-commerce website such as an online store, a telecommunications company or a credit card company. According to the Japan Consumer Credit Association, loss from unauthorized use of credit cards by criminals who stole card numbers was approximately 31.2 billion yen (up 39.4% from the previous year) and has increased compared to the previous year[*5]. It is believed that the target of phishing attacks has shifted from financial institutions to e-commerce and credit card companies.

Table 2 [Number of Reports on Phishing]

	2017	2018	2019	2020	2021
Number of Reports	9,812	19,960	55,787	224,676	526,504

*1 "Cashless payment ratio" means the cashless payment ratio in 2021 on the website of the Ministry of Economy, Trade and Industry.

*2 Violation of the Act on Prohibition of Unauthorized Computer Access, offences involving computers or electromagnetic records and other offences using advanced information and telecommunications networks as means necessary for committing crimes.

*3 "2021/12 Status of Reports on Phishing" on the website of the Council of Anti-Phishing Japan and other information.

*4 "Changes in Targets of Phishing Attacks" on the website of the Japan Cybercrime Control Center (JC3).

*5 "March 2022 Report on Loss from Unauthorized Use of Credit Cards" on the website of the Japan Consumer Credit Association

The number of ransomware attack cases[*1] reported to the National Police Agency in 2021 was 146 cases, and this number has continued to increase as in the previous year. Ransomware attacks affected all kinds of companies and organizations, regardless of the size and industry type (see Table 3). In some cases, restoring an infected system, etc. took two or more months, or cost 50 million yen or more to investigate and restore. In another case, a system for electronic health records at a medical institution in Japan was infected with ransomware, resulting in temporary suspension of new patient registration and emergency medical services. There were cases in which civic life was significantly affected because critical infrastructure companies were targeted by ransomware. The following are characteristics of victims of ransomware attacks:

○ Many of them were victims of double-extortion[*2].

The police were able to figure out the modus operandi used by criminals to demand money in 97 of all 146 cases of ransomware attacks, and 82 cases of those involved double-extortion, accounting for 85%.

○ In many cases, criminals demanded money in crypto-assets.

In 45 cases of all 146 cases, criminals directly demanded money from victims, and in 41 of those cases, criminals demanded money in crypto-assets, accounting for 91%.

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

Looking at the cases of ransomware attacks (146 cases) by the size of companies and organizations, etc.[*3], in 49 cases, the victims were large companies, and in 79 cases, the victims were small and medium-sized ones. In this way, ransomware attacks caused damage to companies regardless of their size.

Ransomware attacks, such as the one targeting an oil pipeline company in the U.S. that occurred in May 2021, can significantly affect civic life around the world, so strong international collaboration is necessary to combat such attacks. Implementing measures to prevent ransomware attacks has become an urgent task worldwide, and an example of doing so was the G7 Interior and Security Senior Officials' Extraordinary Forum on Ransomware, attended by the LEAs of G7 countries, etc. that took place in December 2021.

Table 3 [Number of Reports on Ransomware Attacks Submitted by Companies and Organizations, etc.]

	Second Half of 2020	First Half of 2021	Second Half of 2021
Number of Reports	21	61	85

In addition, cyberattacks conducted to steal information occur frequently, and the number of accesses considered to be search activities in cyberspace detected by the National Police Agency is also increasing. Thus, the threat in cyberspace has become a serious issue in Japan.

(2) Terrorism Situation

As for 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. Since the U.S. forces stationed in Afghanistan were withdrawn at the end of August 2021, we must pay close attention to changes in terrorism threats inside and outside of Afghanistan. Terrorist attacks occurred one after another in various parts of the world, and there were also cases in which Japanese people and interests of Japan were targeted overseas by terrorism. As such, the threat of terrorism against Japan still exists. Although many years have passed since abduction by North Korea occurred, not all victims have yet return to Japan. There is no time to lose before resolving this issue.

---

*1 "Ransomware" means an illegal program for encrypting data stored in infected devices, etc. to demand money for decoding the data made unusable by the program.

*2 "Double-extortion" means that criminals demand money from companies, etc. after encrypting and stealing data from them by saying "the data will be disclosed if payment is not made."

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

*4 First letters of Islamic State of Iraq and the Levant, the so-called Islamic State (or IS). Although ISIL used to be a group affiliated with AQ, it separated from AQ due to policy differences. The group took control of Mosul, a city in northern Iraq, in June 2014 and expanded the areas under its control before declaring the establishment of the Islamic State in areas straddling Iraq and Syria. Many extremist groups in North and West Africa and Southeast Asia have sympathized with ISIL's propaganda and expressed their support and loyalty to ISIL.

*5 Abbreviation for Al-Qaeda

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.

Section 3. Analysis of Money Laundering Cases, etc.

1. Offenders

Although there are various types of perpetrators of money laundering, Boryokudan (Japanese organized-crime groups), fraud (phone scam) groups, and crime 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[*1] in 2021, 64 cases (10.1%) were related to Boryokudan members, associates and other related parties (hereinafter referred to as "Boryokudan gangsters") (see Table 4). Out of those, 60 cases involved violation of the Act on Punishment of Organized Crimes (32 cases of concealment of criminal proceeds and 28 cases of receipt of criminal proceeds) and 4 cases involved violation of the Anti-Drug Special Provisions Law (2 cases of concealment of illegal drug proceeds and 2 cases of receipt of illegal drug proceeds).

When looking at the number of cleared cases of money laundering between 2019 and 2021 in which Boryokudan gangsters were involved in relation to predicate offenses, the majority was fraud and loan shark.[*2]

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 the U.S., the "Strategy to Combat Transnational Organized Crime" was published and a Presidential executive order[*3] was enacted in July 2011. In them, the U.S. designated 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 4 [Number of Cleared Money laundering Cases (Committed by Boryokudan Gangsters) under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law]

Category \ Year	2019	2020	2021
Cleared cases of money laundering offenses	537	600	632
Cases by Boryokudan gangsters	58	58	64
Percent (%)	10.8%	9.7%	10.1%

*1 Meaning the offenses 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 offenses (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 (offenses related to (high interest rate, etc.)) and offenses 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 Executive Order 13581 of July 24,2011

(2) Fraud (phone scam) Group

In recent years, the number of recognized fraud (phone scam) cases and the amount of loss suffered have remained high (see Table 5). Victims were geographically concentrated in metropolitan areas. The numbers of fraud (phone scam) cases recognized in 2021 were 3,319 cases in Tokyo, 1,538 cases in Osaka, 1,461 cases in Kanagawa, 1,103 cases in Chiba, 1,082 cases in Saitama, 874 cases in Aichi and 859 cases in Hyogo. The cases recognized in these seven prefectures accounted for 70.6% of the total number of cases recognized. Having the ringleader as the core, fraud (phone scam) groups assign a role to each member. For example, one-member cheats victims, another withdraws money, and the other procures tools to commit the crime by skillfully abusing various means, including deposit and savings accounts, mobile phones, and call forwarding services. In this way, they commit organized fraud. In addition, they launder money, for example, by using bank accounts in the name of fictitious or third parties as a means to receive money from a victim. Crime bases have spread to rental condominiums, rental offices, vacation rentals, hotels and vehicles. Foreign crime bases have also been found to exist.

In some cases, providers of services abused for fraud (phone scam) were proactively involved in fraud (phone scam) offences. For example, there was a case in which a telephone forwarding service provider provided an Internet Protocol telephone service, knowing that the service would be used by a fraud (phone scam) group. Another case involved a telephone forwarding service provider selling electronic money stolen in collusion with a fraud (phone scam) group through fraud (phone scam) to buyers, and making the buyers transfer payments for the electronic money to another telephone forwarding service provider's personal account.

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.

At the Ministerial Meeting Concerning Measures Against Crime held on June 25, 2019, "It's me fraud countermeasure plan" was decided as a comprehensive measure to protect the elderly from fraud (phone scam). Based on this, the police are promoting various measures to eradicate fraud (phone scam) in cooperation with related government agencies and businesses. While reinforcing guidance and supervision for specified businesses that operate telephone forwarding services used for crimes, the police cleared electronic money purchasers in violation of the Act on Punishment of Organized Crimes and Control of Crime Proceeds.

Table 5 [Number of Recognized Fraud (phone scam) Cases and Total Financial Damage]

Year / Category	2019	2020	2021
Number of recognized cases	16,851	13,550	14,498
Total financial damage (yen) (Effective total amount of financial damage)	31,582,937,585	28,523,359,039	28,199,462,547

Note 1: Data from the National Police Agency

2: The effective total amount of financial damage means original damage from fraud plus money that was withdrawn from ATMs by the use of defrauded or stolen cash cards (aggregate value from the statistics based on surveys, etc. conducted by the National Police Agency).

(3) Crime groups of foreigners in Japan

Criminal proceeds from offenses 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 fact that their human networks, mode of committing offenses, 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 criminal groups existing in their home countries, and these offenses 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 2021, 91 cases (14.4%) were committed by foreigners in Japan (see Table 6). The breakdown comprised 60 cases of concealment of criminal proceeds, and 31 cases of receipt of criminal proceeds.

Table 6 [Number of Cleared-Money Laundering Cases (Committed by Foreigners in Japan) under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law]

Category \ Year	2019	2020	2021
Cleared cases of money laundering offenses	537	600	632
Cases by foreigners	71	79	91
Percent (%)	13.2%	13.2%	14.4%

Concerning the cleared cases of money laundering under the Act on Punishment of Organized Crimes in the last three years, China[*1] and Vietnam have been the top two countries of origin of arrested offenders. Chinese criminals comprised approximately half of the total.

Observations of the situation indicate that foreigners in Japan who are involved in organized crime commit money laundering as part of their criminal activities. For instance, there were money laundering cases associated with a group of Chinese stole goods by impersonating a card holder with an unlawfully obtained credit card information and forwarded the goods to an offender who disposed of the goods, etc., a case of shoplifting by a group of Vietnamese, and a case of international fraud by a group of Nigerians.

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:

*1 In this NRA-FUR, “China” does not include “Taiwan,” “Hong Kong Special Administrative Region” and “Macau Special Administrative Region,” unless otherwise specifically stated.

[Recent Situation concerning Crimes Committed by Foreigners in Japan]

Although the total number of cleared cases involving foreigners (the numbers of cleared cases of Penal Code offenses and special law offences) as well as the number of offenders arrested (the numbers of offenders arrested for Penal Code offences and special law offences) have remained relatively stable in recent years, both the number of cleared cases and number of offenders arrested decreased in 2021 compared to the previous year. 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. In terms of the total number of offenders arrested in 2021 (10,677) by nationality and region, Vietnamese accounted for 37.5% (4,007), followed by Chinese 21.6% (2,305), Filipinos 6.5% (695), Brazilians 4.6% (496), and Thais 3.6% (389). As for the total number of offenders arrested by type of crime and violated laws and regulations, violations of the Immigration Control Act and thefts accounted for the highest percentage.

The total amount of loss from offences against property by foreigners in Japan arrested in 2021 was about 2.5 billion yen, of which about 1.5 billion yen (62.5%) was from theft, and about 0.8 billion yen (30.9%) was from intellectual crimes.

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. Regarding violations of the Immigration Control Act, there are many cases in which foreigners with the status of residence of “Technical Intern Training” illegally remain in Japan for work beyond the authorized period of stay or pretend to be legal residents by obtaining a fake residence card after their authorized period of stay has expired.

In many cases, Chinese criminal organizations form groups by using people in local communities or relatives or by inviting colleagues at work. There are also groups such as the Chinese Dragons, which are mainly comprised of descendants of Japanese orphans left behind in China. On the other hand, it has been found in recent years that these groups recruited Chinese and other foreigners remaining in Japan through social media, etc. to have them involved in crime. In the cases of residence card forgery offences, the manufacturing bases that used to exist in China have been moved to Japan, and Chinese and other foreigners remaining in Japan manufacture forged residence cards together with various nationalities in Japan by following the instructions of leaders in China. Since the leaders remain in China, even if a manufacturing base is uncovered, they can recruit Chinese and other foreigners remaining in Japan again to establish a new manufacturing base by the same method. In this way, residence card forgery offences are well organized.

In terms of the number of cleared money laundering cases by nationality over the last three years, Chinese and Vietnamese are also ranked high. The major cleared cases of money laundering involving Chinese, Vietnamese and other foreigners in Japan are as follows:

1. Examples of money laundering cases involving Chinese nationals:

- An offender received goods that were purchased with unlawfully obtained credit card information by impersonating a card holder.
- An offender received proceeds from credit card payments at an unlicensed adult-entertainment business by making the payments transferred to a bank account under another person’s name.
- An offender received criminal proceeds obtained through providing a place for prostitution by making the payments transferred to a bank account under another person’s name.
- An offender sold counterfeit goods by using a cash-on-delivery service and made the payments transferred to a bank account under another person’s name to receive criminal proceeds from the sale.

2. Examples of money laundering cases involving Vietnamese nationals:

- An offender operated an underground bank by accepting requests to remit money overseas through social media and then having customers transfer money to an account opened in Japan under another person’s name.
- An offender received proceeds from the sale of forged residence cards, etc. by having buyers transfer payments to a bank account under another person’s name.

- ○ An offender sent stolen cosmetics and other goods by giving fake names of goods or sender on a shipping label when sending them to another offender who disposed of the goods, etc.

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 another person's name.
- ○ Sri Lankans received compensation for serving as intermediaries for fake marriages by making the payments transferred to a bank account under another person's name.

2. Modus Operandi

(1) Predicate Offenses

In the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Law, the concealment and receipt of proceeds obtained from certain predicate offenses, 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 offenses. Predicate offences include offenses that generate illegal proceeds and those subject to the death penalty, imprisonment with labor for life or four years or longer, or imprisonment without labor, offenses listed in Tables 1 and 2 attached to the Act on Punishment of Organized Crimes, and drug-related offenses listed in the Anti-Drug Special Provisions Law.

The number of cleared money laundering cases categorized as predicate offences in 2019–2021[*1] is as follows (see Table 7):

Table 7 [Numbers and Ratios of Cleared Money Laundering Cases under the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Law, Categorized by Predicate Offense]

Predicate Offenses	Theft	Fraud	Computer fraud	Violation of the Investment Act/Money Lending Business Act	Violation of the Immigration Control and Refugee Recognition Act	Habitual gambling/running a gambling venue for profit	Violation of the Amusement Business Act	Violation of the Anti-Prostitution Act	Violation of the Trademark Act	Drug-related offences	Embezzlement	Extortion	Distribution of obscene material, etc.	Document forgery offenses	Armed robbery	Unauthorized creation of private electromagnetic records	Others	Total
Number of cases	650	604	145	82	43	37	27	23	22	22	21	19	18	17	15	11	62	1,818
Ratio (%)	35.8	33.2	8.0	4.5	2.4	2.0	1.5	1.3	1.2	1.2	1.2	1.0	1.0	0.9	0.8	0.6	3.4	100

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

The size of generated criminal proceeds, relevance to money laundering offenses, etc., types of misused transactions, danger of fomenting organized crime, impact on sound economic activities, etc. differ depending on the type of predicate offense.

It was found that Boryokudan or international crime organizations were involved in some of the predicate offences. Major predicate offenses are analyzed below.

*1 There were 1,769 cleared cases of money laundering under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law from 2019 to 2021. On the other hand, the total number of cleared money laundering cases counted by predicate offenses was 1,818 (See Table 7) because some money laundering cases can be counted in multiple predicate offenses.

(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, but there are also cases in which theft is committed continuously and repeatedly by criminal organizations such as Boryokudan and criminal groups of foreigners in Japan that results in large amounts of criminal proceeds. The total financial damages from theft during 2021 was about 47.4 billion yen (about 15.5 billion yen for the total amount of damage in cash), generating a large amount of criminal proceeds.

(B) Money laundering cases

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

- Cases of buying and keeping stolen cars knowing that they were stolen;
- Cases where an offender used a flea market app to sell stolen goods in another person's name and made buyers transfer payments to a bank account under another person's name;
- Cases where a group of Chinese, etc. purchased goods on the Internet using credit cards obtained illegally, and received the goods by designating addresses of fictitious persons or addresses different from the actual place of residence;
- 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; and
- Cases where an offender withdrew and stole cash by using an illegally obtained cash card and hid the cash in a coin-operated locker.

(ⅱ) Fraud

(A) Forms of offences and criminal proceeds

Fraud offenses, including fraud (phone scam) offenses, have been repeatedly and continuously committed by domestic and foreign criminal groups. Large amounts of criminal proceeds were generated through the use of bank accounts under the name of fictitious persons or other parties and transactions by a legal person disguised to appear as legitimate. The total financial damages from fraud offenses in 2021 was about 76.3 billion yen (Total damages in cash were about 70.8 billion yen). Although the number of cases from theft offenses exceed those from fraud offenses, the average financial damage due to each case of fraud is about 2.29 million yen bigger than that of a theft offense (about 120,000 yen). In particular, fraud (phone scam) offenses generate a large amount of criminal proceeds with an average about 2.02 million yen per case.

(B) Money laundering cases

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

- Cases where an offender misused accounts under the names of individuals sold to crime groups when foreigners left Japan as accounts for receiving money stolen through fraud (phone scam);
- Cases where an offender opened and misused business accounts under the names of fake companies established for receiving proceeds from fraud (phone scam) or fraud targeting public benefits; and
- Cases where an offender opened and misused accounts under fictitious names to receive proceeds from fraud.

In many cases, loss from fraud offenses were transferred to bank accounts under the name of fictitious or other parties. In addition, there is a tendency that the criminal proceeds transferred to such accounts are withdrawn by offenders immediately after the transfer, remitted to other accounts, transferred through multiple accounts opened under borrowed names or transferred to crypto-asset accounts. This is to prevent financial institutions or the like from freezing the accounts when they discover the loss. Holders of accounts used for concealment differ depending on the form of the offense; they may be individual persons, corporate bodies, or individual persons accompanied by a business name.

There were also cases where business operators of postal receiving services or call forwarding services did not sufficiently follow their customer verification obligations, and as a result were misused as a way to conceal crime organizations committing fraud (phone scam) offenses, etc.

(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 others to accounts managed by the offenders. Some of the cash cards used in computer fraud were illegally obtained through fraud (phone scam). Losses due to online banking fraud in 2021 was approximately 820 million yen. Looking at such accounts by the nationality of account holders, the percentage of Japanese account holders was the highest, accounting for 30.7%, followed by Vietnamese, accounting for 28.9% and Chinese, accounting for 6.4%.

(B) Money laundering cases

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

- Cases where the maximum amount of cash was withdrawn from ATMs using cash cards obtained via fraud (phone scam) offenses, and the maximum amount for transfer was illegally remitted to accounts under the name of another person managed by the criminals from the accounts of the victims;
- 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 another person's name managed by the offenders to allow a Chinese criminal group in Japan to withdraw cash from the account; and
- 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.

(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 another 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. In recent years, there have been cases called "salary factoring," etc. where offenders, who are not registered to operate a money lending business, purchase salary claims held by individuals (workers) against employers and provide them with money to collect funds related to the claims through such individuals. There have also 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. The amount of loss from loan-shark crime committed by offenders who were arrested in 2021 exceeded 9.4 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 a predicate offence include the following cases:

- Cases where debt repayments were remitted to accounts under the name of other parties to conceal debt repayments to the loan sharks; and
- Cases where an offender made use of credit card payment to require 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 where:

- loan sharks required borrowers to send repayments to a post-office box opened under the name of another individual 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 another person; and
- loan sharks made a borrower transfer repayments to another borrower's account and made the second borrower send all or part of the repayments to another 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 (hereinafter referred to as "possession of a forged residence card, etc."); 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 2021, there was a case where approximately 58 million yen of bank deposit claims for compensation for temporary employment became subject to confiscation and non-penal confiscation due to violation of the Immigration Control Act, in which offenders made foreigners in Japan undertake illegal employment.

(B) Money laundering cases

Money laundering offences involving 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 another person's name; and

- Cases where an offender received compensation for introducing foreigners remaining in Japan after the expiration of their authorized period of stay to employers 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 offenses related to habitual gambling and running a gambling venue for profit, there are various forms of gambling offenses, 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 offenses, 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 2021, the orders for confiscation were issued against about 55 million yen in cash, which was the proceeds from running a gambling venue 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 offense was committed in an online casino in which money bet by customers had to be paid to an account opened under another person's name; and
- Cases where an offender made persons engaging in baseball gambling, etc. transfer dividends to an account under the name of another person.

In addition, there was a case where criminal proceeds obtained via gambling offenses 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 offenses such as violations of the Amusement Business Act or the Anti-Prostitution Act, the reality is that Boryokudan have been directly or indirectly involved in 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 offenses 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 2021, there was a case where bank deposit claims of approximately 11 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 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 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 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

Regarding stimulant-related offences, which account for about 60% of all drug-related offences, in 2021, both the quantity of trafficked stimulants seized (688.8 kg) and the quantity of stimulants seized during attempts to smuggle them (673.1 kg) increased substantially 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 (455), the number of Boryokudan gangsters, etc. arrested was 246, accounting for 54.1%. The situation that Boryokudan is deeply involved in smuggling and illicit trafficking of stimulants has continued.

Cannabis-related offences account for about 40% of all drug-related offences, which is the second highest percentage following stimulant-related offences. This percentage has been increasing since 2013; in particular, the number of young people arrested increased. In 2021, the quantity of dried cannabis seized (329.7 kg) increased. In addition, a large quantity of cannabis concentrates for electronic cigarettes, etc. seized (22.2 kg) and a large quantity of smuggled cannabis concentrates (18.3 kg) reach high in 2021.

The number of Boryokudan gangsters arrested for making profits from cannabis was 104, accounting for 24.4% of the total number of offenders arrested for making profits from cannabis (426). 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 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.

The breakdown of cleared cases of drug smuggling offences in 2021 by source country and region indicates that Mexico was the major source country of stimulants, followed by Thailand, the U.S., Malaysia and the U.K., and the U.S. was the major source country of cannabis, followed by Vietnam, the U.K., Thailand and Canada. The breakdown of foreigners in Japan arrested for offences related to drug trafficking in 2021 by nationality, etc. indicates that the number of Vietnamese arrested for trafficking of stimulants was the largest, followed by Iranians, Brazilians, South Koreans and Filipinos, and the number of Vietnamese arrested for trafficking of cannabis was the largest, followed by Brazilians and South Koreans.

As described above, criminals are likely to move criminal proceeds related to trafficking or smuggling of drugs between countries that have different legal and transaction systems.

The number of cases of temporary restraining order for confiscation before institution of prosecution prescribed by the Anti-Drug Special Provisions Law in 2021 was 24, and the sum of monetary claims subject to the orders was about 32.7 million yen. In addition to monetary claims, properties that became subject to temporary restraining order for confiscation before institution of prosecution prescribed by the Anti-Drug Special Provisions Law in the past included vehicles, land and 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 another person's name; 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 these cases where offenders concealed and received criminal proceeds as payments at a bank account under another person's name, there were cases where offenders misused payment systems for flea market apps to disguise reasons for receiving payments.

[Money Laundering Related to Environmental Crimes]

1. FATF Report

In the report published in July 2021*1, FATF stated that there is no universally accepted definition of environmental crime; however, FATF mentioned that environmental crimes such as the illegal sale and purchase of wild fauna and flora, forest resources or minerals and illegal waste disposal are highly profitable offences that generate about 110 billion to 281 billion dollars every year and are linked to many other serious organized crimes such as corruption, tax evasion and drug dealing.

The above report analyzes cases of environmental crimes and indicates that environmental crimes have the following characteristics:

○ They use a front company to co-mingle criminal proceeds with legitimate proceeds;

○ They use a shell company to hide their beneficial owner;

○ They disguise movement of criminal proceeds as legitimate trade; and

○ They misuse financial institutions, etc. to move criminal proceeds, etc.

The report also lists the following three goals for each country to prioritize in order to combat money laundering related to environmental crimes:

(i) All countries, including those without natural resources industries, need to pay attention to the threats of money laundering;

(ii) Each country needs to fully comply with the AML standards as required by FATF; and

(iii) Each country should strengthen public-private partnerships to share risk awareness.

2. Environmental Crimes in Japan

Environmental crimes in Japan include illegal waste disposal and wildlife-related offences. The number of cleared cases of environmental crimes between 2019 and 2021 is as follows:

	2019	2020	2021
Illegal waste disposal	5,375	5,759	5,772
(of which are illegal industrial waste disposal from among the above)	706	801	760
Environmental crimes other than the above	814	890	855
Total	6,189	6,649	6,627

Note 1: According to "Cleared Cases of Offences under the Supervision of the Director for Economic Crime Investigations, Community Safety Bureau, National Police Agency in 2021," published by the National Police Agency.

2: "Environmental crimes other than the above" includes violation of the Forest Act, the Construction Material Recycling Act, the Water Pollution Prevention Act, etc., as well as wildlife related offences such as violation of the Act on Welfare and Management of Animals and the Wildlife Protection, Control, and Hunting Management Act.

There were not as many cleared cases of money laundering offences involving environmental crimes as a predicate offence as those involving theft or fraud as a predicate offence. However, there was a case where an offender who provided services to dispose of industrial waste without a license received criminal proceeds by making customers pay for services to transport industrial waste generated from demolition work by transfer to a bank account under another person's name.

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

We analyzed cleared cases of money laundering (3 years from 2019 to 2021) and counted the detected transactions, etc. to be misused for money laundering while conducting criminal investigations[*2].

*1 Money Laundering from Environmental Crime (July 2021)

*2 This Assessment Report takes transactions, etc. misused for concealing/receiving criminal proceeds, plus transactions, etc. utilized for transforming criminal proceeds, as targets for analysis.

There were 478 cases of domestic exchange transactions[*1], 253 cases of cash transactions and 167 cases of deposit transactions that were misused of money laundering. They accounted for the majority of the transactions misused for money laundering (see Table 8).

Table 8 [Major Transactions, etc. Misused for Money Laundering]

Misused transactions / Year	Domestic exchange transactions	Cash transactions	Deposit transactions	Credit card	Electronic money	Legal persons	Crypto-assets	International transactions (such as foreign exchanges)	Funds transfer services	Precious metals and stones	Postal receiving service	Legal/accounting professionals	Foreign Currency Exchanges	Financial instruments	Total (Number of cases)
2019	160	61	31	15	12	14	2	14	6	3	3	1	0	0	322
2020	110	120	96	20	12	14	32	16	1	2	0	1	1	0	425
2021	208	72	40	40	23	16	9	9	9	2	0	1	1	2	432
Total (Number of cases)	478	253	167	75	47	44	43	39	16	7	3	3	2	2	1,179

Through analyzing cleared cases of money laundering and STRs, we found that 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. Such criminal proceeds are often ultimately withdrawn from ATMs, making it very difficult to track the funds.

It is therefore recognized that domestic exchange transactions, cash transactions, and deposit transactions are misused in many cases for money laundering in Japan.

Typical examples of misused transactions, etc. are:

- ○ Transferring criminal proceeds from fraud to accounts in the name of another party (Domestic exchange transactions)
- ○ Converting stolen goods from theft offenses into cash by selling them in the name of another party (Cash transactions)
- ○ Depositing stolen cash into accounts in the name of another party (Deposit transactions)
- ○ Using illegally obtained credit cards (information) to purchase goods by impersonating card holders (Credit card)
- ○ Remitting criminal proceeds from fraud to accounts of dummy corporations (Legal persons[*2])
- ○ Depositing money obtained from victims by fraud in a crypto-asset account under another person's name to purchase crypto-assets and send them to anther account (crypto-assets)
- ○ Remitting criminal proceeds from fraud from a foreign country to an account in Japan (Transactions with a foreign country)

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

*2 With respect to the details of cases where legal personality was misused, this NRA-FUR also explains the results of surveys and analyses in "Legal Persons (Legal Persons without Transparency of Beneficial Owner, etc.)" under *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes*.

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, and certified public tax accountants) to submit suspicious transaction reports to competent authorities if assets received in specified business affairs[*1] 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 submitted in 2021 by business type reported by competent authorities, the percentage of STRs submitted by banks and other deposit-taking institutions was the largest, accounting for 77.7% (411,683) of the total STRs, followed by money-lending companies at 6.7% (35,442) and credit card companies at 6.6% (34,904) (see Table 9).

The number of STRs used for the investigation, etc. by the prefectural police in 2021 was 353,832 (see Table 10).

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

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

Table 9 [Number of STRs by Business Type Reported by Competent Authorities]

Category \ Year	2019	2020	2021
	Number of reports	Number of reports	Number of reports
Financial institutions, etc.	415,299	402,868	495,029
Deposit-taking institutions	366,973	342,226	411,683
Banks, etc.	344,523	319,812	390,381
Shinkin Banks, Credit Cooperative	19,487	19,793	18,461
Labour Banks	371	300	318
Norinchukin Banks, etc.	2,592	2,321	2,523
Insurance Companies	2,876	2,635	3,458
Financial Instruments Business Operators	17,116	17,933	19,718
Money Lenders	17,316	25,255	35,442
Fund Transfer Service Providers	3,913	6,040	10,499
Crypto-assets Exchange Service Providers	5,996	8,023	13,540
Commodity Derivatives Business Operators	256	320	388
Currency Exchange Operators	712	252	201
Electronic Monetary Claim Recording Institutions	4	5	7
Others	137	179	93
Financial Leasing Operators	270	123	163
Credit Card Operators	24,691	29,138	34,904
Real Estate Brokers	6	7	4
Dealers in Precious Metals and Stones	217	63	48
Postal Receiving Service Providers	4	2	0
Telephone Receiving Service Providers	0	0	0
Telephone Forwarding Service Providers	5	1	2
Total	440,492	432,202	530,150

Table 10 [Number of STRs Used for Investigative Purposes, etc.]

	2019	2020	2021
Number of STRs used in investigation	307,786	325,643	353,832

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

* There are cases where the content of a report is not directly related to the name of the change in a cleared case.

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

(1) Deposit-taking institutions, money lenders, and crypto-asset exchange service providers submitted STRs concerning accounts of Japanese people or contracts (including those that were declined) for the following reasons such as:

- ○ There were multiple logins from different locations within a short period of time, which is almost impossible due to the distance;
- ○ It is suspected that a third party illegally sent crypto-assets by impersonating another person or using funds of a person other than the sender;
- ○ It is suspected that a fictitious or another person's name was used;
- ○ A security camera captured a person other than an account holder using an ATM; or
- ○ An account holder notified that he/she had discovered fraud.

Through the STRs submitted for the above reasons, etc., it was discovered that third parties illegally opened some accounts for receiving governmental funds in fraud cases. The users of those accounts were arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

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

- ○ A large amount of money was sent to an account with old and not-updated customer information in a foreign country;
- ○ A fund transfer in an unusually large amount was made or a fund transfer in a large amount from a foreign country was made;
- ○ A sender explained that a funds transfer from a foreign country is for legal dealings; however, there was no document that proved such explanation;
- ○ A sender's bank in a foreign country reported that a transaction was a scam and requested the funds to be returned;
- ○ It is suspected that an account holder is an anti-social force and used an account for fraud in a foreign country; and
- ○ An account holder is on the list of account holders subject to account-freezing orders.

Through the STRs submitted for the above reasons, etc., it was discovered that some accounts were used in international fraud cases. Criminals involved in the fraud cases, including holders of such accounts, were arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

2. Fraud Cases

(1) Deposit-taking institutions, insurance companies, currency exchange operators, and credit card operators submitted STRs concerning accounts of Japanese people or contracts for the following reasons such as:

- ○ It is suspected that a customer made a transaction in an amount slightly less than the amount of transaction categorized as a specified transaction to avoid identity verification;
- ○ Even though an account is used as a living expense account, government funds for business operators are deposited into the account, and the details of the business are obscure; and
- ○ Transactions involve Boryokudan or persons affiliated with Boryokudan, etc.

Through the STRs submitted for the above reasons, etc., it was discovered that holders of the accounts (Boryokudan members) had illegally received government funds multiple times, and such holders were arrested for fraud.

(2) Deposit-taking institutions, financial instruments business operators, crypto-asset exchange service providers, and commodity derivatives business operators submitted STRs concerning accounts of Japanese people or contracts for the following reasons such as:

- An account holder frequently received funds from many senders without good reason;
- An account holder changed his/her login authentication method and password of his/her account for crypto-asset transactions immediately before depositing money in a crypto-asset account, purchased crypto-assets after depositing money and transferred the crypto-assets to another address, which resembles the characteristics of an illegal transaction;
- It is suspected that an account was used by a third party or for fraud; or
- A case of fraud was notified by a victim.

Through the STRs submitted for the above reasons, etc., it was discovered that users of the above accounts had been engaged in fraud (phone scam) under the name of refunds, and such users were arrested for fraud and violation of the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

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 for the following reasons such as:

- Frequent remittances were made in a short period of time, in which almost the same amount was deposited and withdrawn during a certain period;
- An account holder who is a foreign student frequently received and sent funds from and to many foreigners who do not have specific relationships with the account holder, stating the purpose of transactions as payment for living expenses;
- A transaction deviates from past transaction behavior; and
- A customer whose authorized period of stay in Japan has expired continues to use ATMs and make transactions, and has not followed procedures to update customer information (authorized period of stay).

Through the STRs submitted for the above reasons, etc., it was discovered that some accounts were used by loan sharks targeting foreigners, and the holders of such accounts were arrested for violating the Money Lending Business Act (unregistered business operation) and the Investment Act (high interest rate).

(2) Deposit-taking institutions and crypto-asset exchange service providers submitted STRs concerning accounts of Japanese people and companies for the following reasons such as:

- A small amount of crypto-assets was sent to many people in a very short period of time;
- A large amount of cash was withdrawn after deposits were made by several companies and individuals;
- A customer requested withdrawal of a large amount of funds in cash at a branch located on the second floor or above, at which individual customers are not expected to visit, and the purpose of use of the funds is obscure;
- Funds were transferred from an account suspected of being used for crimes; and
- A case of fraud was notified by a victim.

Through the STRs submitted for the above reasons, etc., it was discovered that several people, including holders of the above accounts, illegally collected funds for investment from many investors, and the account holders were arrested for violating the Investment Act (no receipt of deposits).

4. Narcotics-Related Crimes

(1) A deposit-taking institution submitted STRs concerning accounts of Japanese people for the following reasons such as:

- ○ A customer frequently received funds from several individuals and withdrew funds at an ATM or sent the funds to a third party individual immediately after receiving them;
- ○ A customer frequently engaged in transactions with many people; however, the relationships between them, source of funds or reason of remittances is obscure;
- ○ An account holder who is a minor engaged in transactions with many people, including specific persons, whereby it is suspected that the account is used by a third party; and
- ○ Transactions involved Boryokudan or persons affiliated with Boryokudan, etc.

Through the STRs submitted for the above reasons, etc., it was discovered that there were suspicious funds transfers involving the accounts, the account holder was arrested for violating the Cannabis Control Act (possession of cannabis for profits).

(2) Deposit-taking institutions, money lenders, and credit card operators submitted STRs concerning accounts of Japanese people and contract for the following reasons such as:

- ○ It was discovered from a security camera installed at an ATM that the same account was used by several people;
- ○ Funds were transferred to or from a frozen account that was suspected of being used for crimes in the past;
- ○ Remittances or deposits to or from an account were frequently made by many people, whereby the account was suspected of being used illegally; and
- ○ Transactions involved Boryokudan or persons affiliated with Boryokudan, etc.

Through the STRs submitted for the above reasons, etc., it was discovered that some accounts were used as accounts for collecting criminal proceeds from drug trafficking. The holders of the accounts (Boryokudan members) were arrested for violating the Anti-Drug Special Provisions Law (receipt of criminal proceeds from drugs, etc.), and other persons involved including users of the accounts were arrested for violating the Cannabis Control Act (possession), etc.

5. Case of Violation of the Immigration Control Act

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

- ○ A customer was not able to provide a reasonable explanation when he/she was asked the purpose of opening of an account;
- ○ A transaction deviated from past transaction behavior;
- ○ Funds in large amounts were sent from many individuals in foreign countries, and the funds were transferred to a crypto-asset exchange service provider, or funds were withdrawn in cash immediately after they were received;
- ○ The number of unreasonable transactions increased all of a sudden; and
- ○ A large amount of funds transferred by a crypto-asset exchange service provider multiple times were withdrawn in cash repeatedly.

Through the STRs submitted for the above reasons, etc., it was discovered that an account holder provided false information when following the procedures to renew an authorized period of stay in Japan on behalf of the foreigners, and the account holder was arrested for violating the Immigration Control Act (provision of false information).

(2) A deposit-taking institution submitted STRs concerning accounts of foreigners for the following reasons such as:

- ○ Funds in large amounts were transferred to or from an account between an account holder and many foreigners who do not have specific relationships with the account holder, including persons subject to account freezing orders;
- ○ Funds were sent frequently in a short period of time, and almost the same amount of deposits and withdrawals were made during a certain period;

- ○ An account holder who is a foreign student frequently engaged in transactions with unspecified number of foreigners, and the details and an amount of transactions were contradictory to the attributes of the account holder; and
- ○ An account holder whose authorized period of stay in Japan has expired continued to use ATMs and make transactions, and has not followed the procedures to update customer information (authorized period of stay).

Through the STRs submitted for the above reasons, etc., it was discovered that an account holder possessed a forged residence card, and the account holder was arrested for violating the Immigration Control Act (possession of forged residence card and illegal overstay).

6. Case of Violating the Trademark Act

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

- ○ An account holder received a large amount of funds in exact amounts from multiple persons who do not have specific relationships with the account holder and immediately withdrew funds repeatedly and continuously;
- ○ An amount of payments received by an account holder on a flea market app was significantly large for individual transactions, and the receipt of payments is not compatible with the purpose of opening of the account;
- ○ An account holder deposited funds and immediately withdrew almost all the funds on the next day, and only a small balance remains in the account all the time;
- ○ An account holder collected funds sent from several persons and sent the funds to another individual, intentionally transferred funds through multiple accounts or was otherwise suspected to have engaged in illegal funds transfers; or
- ○ Transactions involved Boryokudan or persons affiliated with Boryokudan, etc.

Through the STRs submitted for the above reasons, etc., it was discovered that several persons involved, including the account holder (Boryokudan member), sold counterfeit goods as a group, and they were arrested for violating the Trademark Act.

7. Case of Violating the Financial Instruments and Exchange Act

Deposit-taking institutions, money lenders, fund transfer business operators, and crypto-asset exchange service providers submitted STRs concerning accounts of Japanese people or contract for the following reasons such as:

- ○ An account holder was found to have frequently sent crypto-assets to an account that was suspected of being used for investment fraud;
- ○ Information on income and assets provided by an account holder deviated from the amount of actual transactions;
- ○ An account holder was found to have been impersonating another person upon inquiry to the account holder;
- ○ An account holder moved crypto-assets between many crypto-asset exchanges frequently to circulate the crypt-assets; or
- ○ A fraud case was notified by an account holder.

Through the STRs submitted for the above reasons, etc., it was discovered that several persons involved including the account holder had encouraged victims to engage in investment without license, and they were arrested for violating the Financial Instruments and Exchange Act (unregistered business).

8. Cases of Violation of Act on Prevention of Transfer of Criminal Proceeds and Other Offences

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

- ○ An account holder received funds from several individuals suddenly after opening an account, and transferred the funds to another person or withdrew the funds at an ATM immediately;
- ○ Sudden multiple withdrawals at an ATM and multiple funds transfers from a remote location occurred on an account that had been inactive for some time;

○ It was found that an account holder received funds from many people multiple times and withdrew the funds or sent the funds to a specific person multiple times immediately after receiving the funds; and

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

Through the STRs submitted for the above reasons, etc., it was discovered that an account holder opened an account for transferring the account, and the account holder was arrested for transfer of an account to a third party in violation of the Act on Prevention of Transfer of Criminal Proceeds, etc.

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

A deposit-taking institution submitted STRs concerning accounts of foreigners for the following reasons such as:

○ Suspicious behavior was observed when an account holder whose account had been inactive for a long time asked to raise the maximum amount of withdrawals;

○ An account holder received funds from unspecified number of individuals and withdrew the funds at an ATM or followed the procedures to send the funds to unspecified number of persons immediately after receiving the funds;

○ A large amount of cash was deposited at an ATM to an account that had been inactive for a long time after a small amount of deposit and withdrawal had been made on the account all of a sudden;

○ An account holder deposited a large amount cash at an ATM and immediately withdrew almost all the funds at an ATM that is far from the ATM where the funds were deposited;

○ A security camera installed at an ATM captured image of a depositor who was found to be different from an account holder; and

○ An account holder frequently transferred and received large amounts of funds to and from many foreigners who do not have specific relationships with the account holder.

Through the STRs submitted for the above reasons, etc., it was discovered that an account holder conducted banking business without license, and the account holder was arrested for violating the Banking Act.

10. Case of Violating the Anti-Prostitution Act

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

○ An account holder deposited a large amount of cash frequently by paying fees at an ATM in a convenience store;

○ An account holder sent funds multiple times under different names after depositing a large amount of cash at an ATM;

○ An account holder received large amounts of funds one after another from a company conducting adult-entertainment business;

○ A business account, which was opened as an account for payment of business expenses, has been inactive; and

○ An account holder was unable to provide reasonable explanations about mail that was undelivered due to an unknown addressee issue.

Through the STRs submitted for the above reasons, it was discovered that several persons involved, including an account holder, provided a place for prostitution, and they were arrested for violating the Anti-Prostitution Act.

[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, etc., and recent crime cases and trends, etc. reported by each investigative organization, etc.[*1] are as follows:

1. Embezzlement in the Pursuit of Social Activities (Public Prosecutors Office)

A deposit-taking institution submitted STRs concerning accounts of Japanese people for the following reasons such as:

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

- ○ 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; and
- ○ 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. Tax Evasion (National Tax Agency)

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

- ○ An account holder deposited a large amount of cash using an unidentified source of funds at a bank teller, and transferred all of the funds to an account under another person's name at a different bank. These were suspicious transactions, considering the account holder's age and other attributes;
- ○ Large amounts of cash were frequently deposited at an ATM; and
- ○ The purpose and source of funds of a large amount of remittance to a foreign country were not identified.

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 2021, the National Tax Agency accused a case for illegal receipt of refund of consumption taxes, etc. (a case of corporation holding pet animal events abused the tax credit system for consumption tax) and non-filing cases (contracting of construction work related to a solar power generation system and mail order of imported goods on an online shopping site, etc.). In addition, the National Tax Agency accused a case for international fraudulent scheme using overseas corporations, and cases in which a former employee of a construction company received reward money from a subcontractor, etc., which have substantial spillover effects on the society. Looking at these cases by type of business, the number of cases involving construction business and real estate business accounts comprised the largest percentage.
- ○ Most of the illegal funds obtained through tax evasion used to be withheld in cash or bank deposits. In some cases, however, such illegal funds were used to invest in real estate or securities, etc., to buy luxury cars or watches, or to pay expenses for amusement such as gambling including overseas casinos and expensive night clubs.

3. Drag Smuggling Cases (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;
- ○ 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; and
- ○ 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. Drug Trafficking Cases (Narcotics Control Department, Regional Bureaus of Health and Welfare, Ministry of Health, Labour and Welfare)

Deposit-taking institutions, credit card operators, crypto-asset exchange service providers, and money lenders submitted STRs concerning accounts of Japanese people for the following reasons such as:

- ○ It was discovered from a security camera installed at an ATM that the same account was used by several persons;
- ○ An account holder withdrew funds immediately after receiving funds from several individuals or companies, transferred funds to several individuals after depositing cash using an unidentified source of funds at an ATM for an unidentified purpose, or otherwise made unusual transactions;
- ○ Large amounts of funds were frequently transferred by unspecified individuals;
- ○ An account holder was on the list of account holders subject to account-freezing orders; and
- ○ There was a suspicious transaction failure in which an account holder asked to change a large amount of cash into new bills without providing requested documents certifying the source of funds, etc. and withdrew the request in the middle of the process.

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, accounts under the names of others are used to receive and conceal criminal proceeds from drugs. In the past, offenders affiliated with drug trafficking groups used accounts of persons who have almost no relationship with them. However, the number of cases in which offenders affiliated with drug trafficking groups use accounts of those who have close relationships with them to respond to inquiries from financial institutions has recently increased. This is because financial institutions enhanced measures to monitor suspicious transactions, i.e., they will suspend deposit transactions or otherwise restrict transactions if an account holder is unable to respond to inquiries about the purpose of transactions, etc.
- ○ When receiving criminal proceeds from drugs in cases of trafficking of controlled substances, a lot of desktop wallets, which can be easily created with a personal computer, etc., are used. Offenders transfer criminal proceeds from drugs by using crypto-asset exchange service providers in foreign countries after receiving the criminal proceeds in crypto-assets in desktop wallets. Since in some cases it is difficult to find the actual location of a crypto-asset exchange service provider, if criminal proceeds are transferred to a crypto-asset exchange service provider in a foreign country, it is extremely difficult to understand the process of transfer of criminal proceeds until they are converted into cash. This is because the country to which a request for international assistance in investigation should be sent cannot be identified.

5. Poaching Cases (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 suspiciously deposited funds at an ATM and withdrew the funds at an ATM that is far away;
- ○ An account holder frequently engaged in transactions in exact amounts with trading companies or specific individuals, which are not considered to be business transactions; or
- ○ An account holder received a large amount of funds from a trading company and sent the total amount of funds to an account of a person affiliated with Boryokudan.

The STRs submitted for the above reasons were utilized to specify the facts about poaching organizations and sales routes, etc.

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

○ There are various forms of 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 indicating that organized poaching has become more invisible and sophisticated, and sales routes have changed. For example, poachers directly sell fish to fishery companies without using a market.

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 offenses, as well as situations that increase the risks of ML/TF (non-face-to-face transactions, businesses that are cash-intensive, etc.) as described in the FATF's Interpretive Notes to the FATF Recommendations, we identified: (1) non-face-to-face transactions; (2) cash-intensive businesses; and (3) international 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 due to the development of information communications technologies, improvement in services of specified business operators that take into account the convenience of customers, and measures for preventing the spread of COVID-19.

For example, deposit-taking institutions provide convenient services where customers can open bank accounts, remit money, or conduct other financial transactions through the Internet. Customers can also use e-commerce services that enable them to apply to open bank accounts by mail. At financial instruments business operators, customers can conduct transactions such as opening securities accounts or share trading through the Internet.

On the other hand, as business operators do not see their customers directly in non-face-to-face transactions, they cannot confirm the customers' sex, age, appearance, behavior, etc. directly and judge if the customers have given false identification data or if they are pretending to be another person. In addition, when a copy of a customer's identification document is used for customer identification, business operators cannot check the feel or texture to confirm whether the document is genuine. These facts show that non-face-to-face transactions may limit measures to detect customers who intend to pretend to be another person, and may reduce the accuracy of customer identification measures. Therefore, compared with face-to-face transactions, non-face-to-face transactions enable offenders to maintain high anonymity, falsify customer identification data such as names and addresses, and pretend to be a fictitious or another person. Specifically, non-face-to-face transactions enable offenders to give false identification data or to pretend to be another person by means such as sending copies of falsified identification documents.

(B) Typologies

The following cases are common examples of misuse of non-face-to-face transactions for money laundering that occurred in 2021:

- A criminal obtained criminal proceeds from benefits fraud related to COVID-19 by impersonating a different person through having the government transfer funds to a bank account, and sent the funds to a bank account under another person's name through an online non-face-to-face transaction.
- 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 another person with a stolen health insurance card, and opened a bank account by using the copy of resident record and health insurance card to transfer funds loaned through an online non-face-to-face transaction to an account opened by impersonating another person.
- A criminal accessed the member website for reserving 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 another person's name through a non-face-to-face transaction.

(ⅱ) Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds and the Ordinance stipulate methods of identity verification of customers, etc. These methods include a method of sending documents related to transactions by registered mail, etc. as non-forwarding mail, etc. or by restricted mail, and a method of completing identity verification online in addition to a method of reviewing identification documents presented by customers, etc. directly to specified business operators.

Furthermore, 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.

Specified business operators also make efforts to mitigate risks by monitoring transactions based on IP addresses and login addresses when determining whether transactions are suspicious or by taking other appropriate measures.

(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 be deteriorated. 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 another person 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

According to the statistics, in 2019 the average monthly consumption expenditure of a household (total household) using cash as the purchasing medium was 174,237 yen (73.5% of all consumption expenditure). For credit card, monthly installment payment, and credit purchases (hereinafter referred to as "credit card, etc."), the average amount was 53,305 yen (22.5% of all consumption expenditure). Although the ratio of expenditure in cash has been declining (82.4% in 2014 and 73.5% in 2019), purchases in cash still comprise the largest proportion of expenditure by means of purchase (see Table 11). Money circulation in Japan is higher than that in other countries (see Table 12).

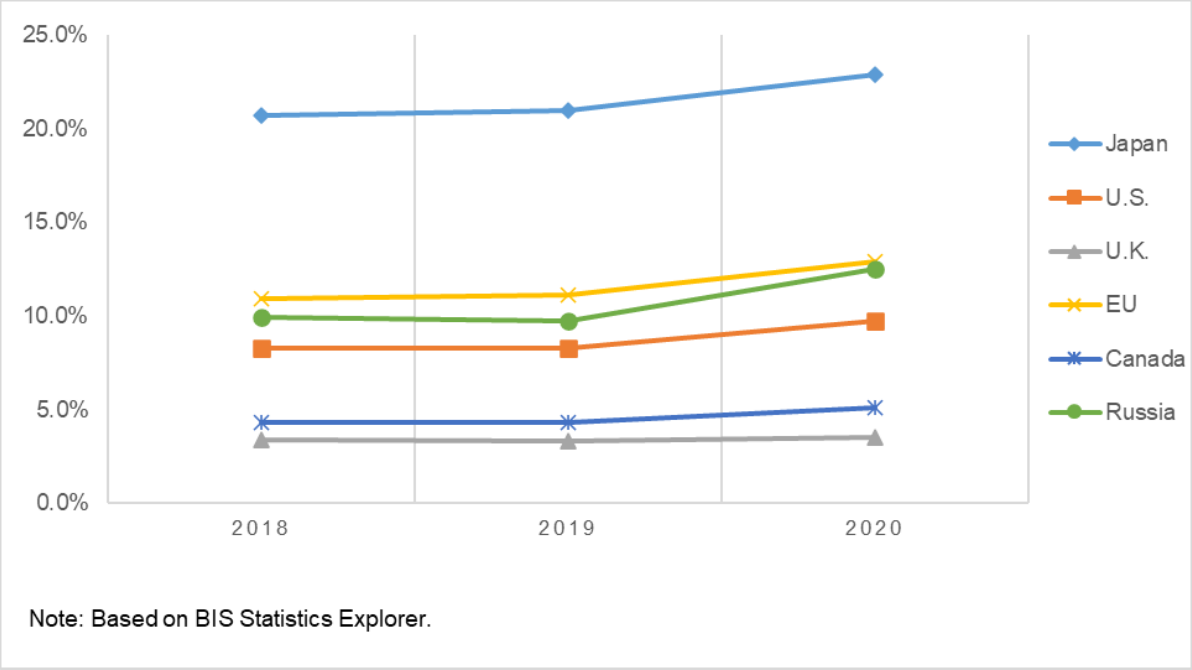
While a reasonable time is necessary for cash transactions because cash is physically transferred, cash transactions are highly anonymous, which is different from foreign/domestic exchange transactions where funds can be transferred to remote locations promptly. Cash transactions are unique in that the flow of funds is not easily traceable unless the transactions are recorded.

Table 11 [Expenditure by Type of Purchase (Total Household/Monthly Average)]

Consumption expenditure	2014				2019			
	Cash	Credit card, etc.	Electronic money	Total	Cash	Credit card, etc.	Electronic money	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 on Household Structure (previous National Survey on Actual Conditions of Consumers) by the Ministry of Internal Affairs and Communications.

Table 12 [Ratio of Cash Distribution Balance for Different Countries in Nominal GDP]



Note: Based on BIS Statistics Explorer.

(B) Typologies

By analyzing cleared cases of money laundering, we found the following cases in Japan:

- Cases where goods obtained by theft or fraud, etc. are converted into cash;
- Cases where criminals receive criminal proceeds by transfer to a bank account under a fictitious or another person's name and convert them into cash at an ATM;
- Cases where criminal organizations, etc. receive criminal proceeds in cash; and
- International money laundering cases where an international criminal organization withdrew a large amount of cash in a single transaction by disguising the legitimacy of transactions, in which criminal proceeds from fraud in a foreign country were sent to a financial institution in Japan.

In these cases, it is difficult to trace the movement of funds due to the existence of cash transactions, and it is recognized that the vulnerability of products and services provided by specified business operators, as well as the liquidity and anonymity, etc. of cash, are misused for ML/TF.

In addition to the above, the following cases are common examples of misuse of cash transactions for money laundering that occurred in 2021:

- Offenders obtained cash by selling or pawning stolen items in the name of a fictitious or another party at secondhand shops, pawnshops, etc.
- Boryokudan gangsters and others received illegal proceeds in cash derived from criminal activities such as prostitution and gambling in the name of protection fees and contributions.
- An offender converted criminal proceeds in cash from robbery into large-denomination bills and also deposited them into a bank account under his/her relative's name.
- An offender received criminal proceeds from fraud (phone scam) or romance fraud, which were transferred to an account under another person' name, and withdrew them in cash at an ATM.

On the other hand, cases where criminal proceeds from money laundering involving cash transactions were confiscated from offenders in 2021 are as follows:

- A penal confiscation order was issued against cash that formed part of payments for illegally obtained cellphones an offender sold to a pawnbroker by impersonating another person with a forged resident card.
- A confiscation order was issued against the total amount of cash deposited in a bank account under another person's name as repayments to a loan shark, which were identified as criminal proceeds, including cash seized by an investigative organization.

(ⅱ) Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds and Ordinance 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 saving verification 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 Articles Dealer Act (Act No. 108 of 1949) and the Pawnbroker Business Act (Act No. 158 of 1950) require the address, name, etc. of the counterparty to be verified at the time of a transaction. As for cash couriers, the FEFTA requires those who export or import the means of payment such as cash etc., exceeding the equivalent of one million yen (100,000 yen in a case bound for North Korea) to notify the Minister of Finance in writing, 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 must be in writing. These measures are considered to t contribute to reducing risks associated with cash transactions.

Furthermore, the Japanese government developed the "Action Plan of the Growth Strategy" (approved by the cabinet on June 18, 2021), etc. to develop a cashless environment. 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.

- Specified business operators consider updating the drafting criteria of the hearing sheet based on the recognized risks, such as multiple transactions at the same store on the same day and transactions at multiple stores.
- Specified business operators refuse overseas remittance transactions by customers whose verification records are not retained because they do not have accounts or for other reasons.

(ⅲ) Assessment of Risks

In general, cash transactions have high liquidity and anonymity. Therefore, cash transactions may hinder the tracing of criminal proceeds unless business operators dealing with cash properly prepare transaction records. 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) International Transactions

(ⅰ) Factors that Increase Risks

(A) Characteristics

With a nominal GDP of approximately 541.4 trillion yen, an overall import value of approximately 84.875 trillion yen and an overall export value of approximately 83.914 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., international 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, so 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 offenses 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 offenses. 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 offenses occur.

Besides the abovementioned exchange transactions, etc. based on correspondent banking relationships, ML/TF by cash couriers could also occur in international transactions.

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 counter 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 oversight by foreign authorities.

(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 in Japan, are involved in such cases. Money laundering is an internationally recognized crime.

The modus operandi used in the above cases include:

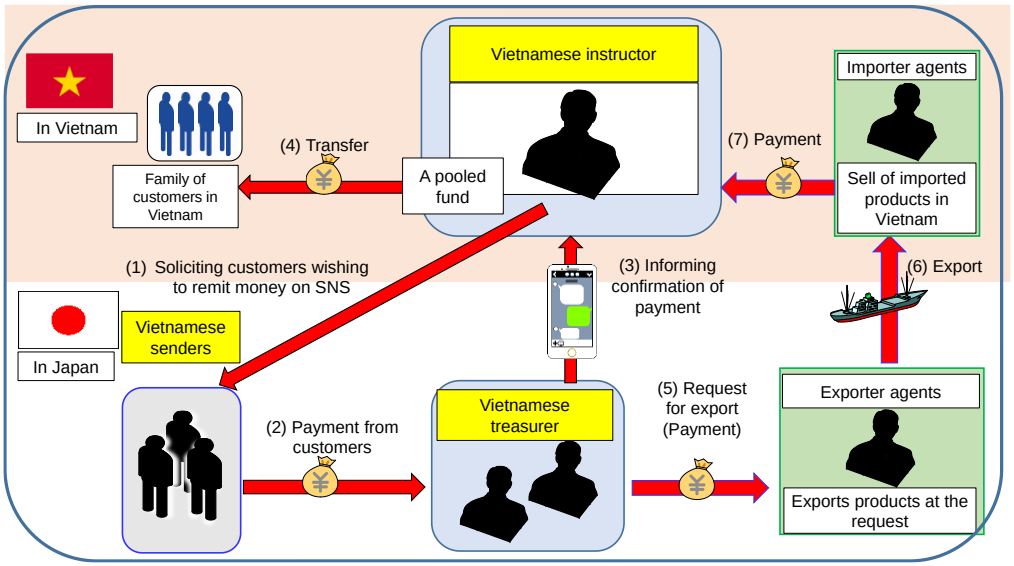
- ○ To misuse financial institutions, etc. in and outside Japan (cross-border remittances, etc.);
- ○ To disguise money laundering as legal trading (export or import of goods, etc.);
- ○ To provide domestic and cross-border remittance and payment services without actually moving funds; and
- ○ To use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

Examples of offences committed through these modus operandi include so-called underground banking (see Table 13).

---

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

Table 13 [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.

Money laundering offences in which cross-border transactions were misused in 2021 include the following cases:

- 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, and 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 another person'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.

(C) Trends of STRs

The number of STRs related to cross-border remittances submitted between 2019 to 2021 was 146,420, and STRs related to transactions to or from China, Hong Kong and the U.S. account for nearly 50% of the total number of such STRs submitted between 2019 to 2021 (see Table 14).

Table 14 [Number of STRs Related to Cross-border Remittances]

Destination (origin) Country or Jurisdiction	2019	2020	2021	Total	Ratio
China	18,425	13,918	11,685	44,028	30.1%
Hong Kong	6,664	5,525	4,848	17,037	11.6%
U.S.	5,596	4,553	4,150	14,299	9.8%
South Korea	2,708	2,429	3,159	8,296	5.7%
Taiwan	2,510	2,208	2,124	6,842	4.7%
U.K.	1,922	1,849	1,684	5,455	3.7%
Singapore	1,639	1,500	1,353	4,492	3.1%
Philippines	1,433	1,208	1,755	4,396	3.0%
Vietnam	1,151	946	1,772	3,869	2.6%
Thailand	1,161	985	780	2,926	2.0%
Other Countries or Jurisdictions	14,032	10,707	10,041	34,780	23.8%
Total	57,241	45,828	43,351	146,420	-

(ⅱ) Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds requires that specified business operators conduct CDD measures and understand 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 an overseas remittance, specified business operators must provide customer identification records of the originator to the institution; and, they must preserve customer identification records provided by a foreign-exchange transaction operator whose country has similar legislation.

Furthermore, 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.

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 one million yen (100,000 yen in a case bound for North Korea), or over 1 kg of precious metals[*2] 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.

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 Foreign Exchange Inspection Guidelines.

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

- To interview corporate customers who start foreign exchange trading, including checks on business details by visiting the corporation
- To reject overseas remittance transactions of customers bringing in cash

*1 Meaning the specified transactions set forth in Article 4.1 of the Act on Prevention of Transfer of Criminal Proceeds.

*2 Of the gold bullions, those with a gold content of 90% or more in the total weight.

- 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

(iii) Assessment of Risks

In transactions with foreign countries, it is difficult 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 international transactions. Therefore, it is recognized that international transactions pose a risk for 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 more sophisticated and latent. There is also a risk that criminal proceeds that are 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
- International 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 an overseas 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.

Particularly regarding 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.

The same request has been made continuously regarding Iran since February 2009. In June 2016, the FATF evaluated the measures taken for 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.

(2) Measures to Mitigate Risks

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

Competent authorities notified specified business operators of the FATF statement and asked 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 file 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 to Iran and North Korea, transactions related to countries and regions mentioned in the FATF statement are required to pay special attention due to the high risks they pose; however, there were no such jurisdictions mentioned in the statement released in June, 2022[*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 that continue to improve the international AML/CFT measures. The FATF is calling on those countries/regions to promptly put those plans into action within the proposed periods of time. Therefore, transactions conducted with those countries/regions before the deficiencies pointed out by FATF are resolved are recognized to be risky. Also, even if there are no direct transactions with these countries, malicious and shrewd methods may be used

*1 See http://www.mof.go.jp/international_policy/convention/fatf/index.html. 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.

to redirect funds through neighboring countries/regions, so thorough measures need to be implemented, including verification at the time of transactions.

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

The following list shows when decisions were made and announced over the last three years (2020 to 2022) regarding the designation of countries/Regions for which FATF requested its members and other jurisdictions to apply counter-measures, etc. in the FATF statements and those designated under the FATF's monitoring process to improve their AML/CFT measures.

Note that the countries/regions announced during the FATF's plenary meeting in June 2022 are listed at the top in alphabetical order, and other countries/regions announced in the past are listed at the bottom, also in alphabetical order.

[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.

Countries/regions and period	2020			2021			2022	
	Feb.	Jun.	Oct.	Feb.	Jun.	Oct.	Mar.	Jun.
Iran	●	●	●	●	●	●	●	●
North Korea	●	●	●	●	●	●	●	●

[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

Countries/regions and period	2020			2021			2022	
	Feb.	Jun.	Oct.	Feb.	Jun.	Oct.	Mar.	Jun.
Albania	○	○	○	○	○	○	○	○
Barbados	○	○	○	○	○	○	○	○
Burkina Faso				○	○	○	○	○
Cambodia	○	○	○	○	○	○	○	○
Cayman Islands				○	○	○	○	○
Gibraltar								○
Haiti					○	○	○	○
Jamaica	○	○	○	○	○	○	○	○
Jordan						○	○	○
Mali						○	○	○
Morocco				○	○	○	○	○
Myanmar	○	○	○	○	○	○	○	○
Nicaragua	○	○	○	○	○	○	○	○
Pakistan	○	○	○	○	○	○	○	○
Panama	○	○	○	○	○	○	○	○
Philippines					○	○	○	○
Senegal				○	○	○	○	○
South Sudan					○	○	○	○
Syria	○	○	○	○	○	○	○	○
Turkey						○	○	○
Uganda	○	○	○	○	○	○	○	○
United Arab Emirates							○	○
Yemen	○	○	○	○	○	○	○	○
Bahama	○	○	○					
Botswana	○	○	○	○	○			
Ghana	○	○	○	○				
Iceland	○	○						
Malta					○	○	○	
Mauritius	○	○	○	○	○			
Mongolia	○	○						
Zimbabwe	○	○	○	○	○	○		

* For the situation in each country, refer to the original text of the statement, “Jurisdictions under Increased Monitoring-June 2022” (https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2022.html).

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) Anti-social forces (including Boryokudan, etc.) and (2) international terrorists (including Islamic extremists)

- ○ Persons for whom it is difficult to conduct CDD

  (3) Non-residents, (4) foreign PEPs, and (5) legal persons (legal persons without transparency of beneficial owner, etc.)

(1) Anti-social Forces (Boryokudan, etc.)

In Japan, Boryokudan and other anti-social forces[*2] 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, 2022, 25 groups are listed as designated Boryokudan under the Anti-Boryokudan Act.

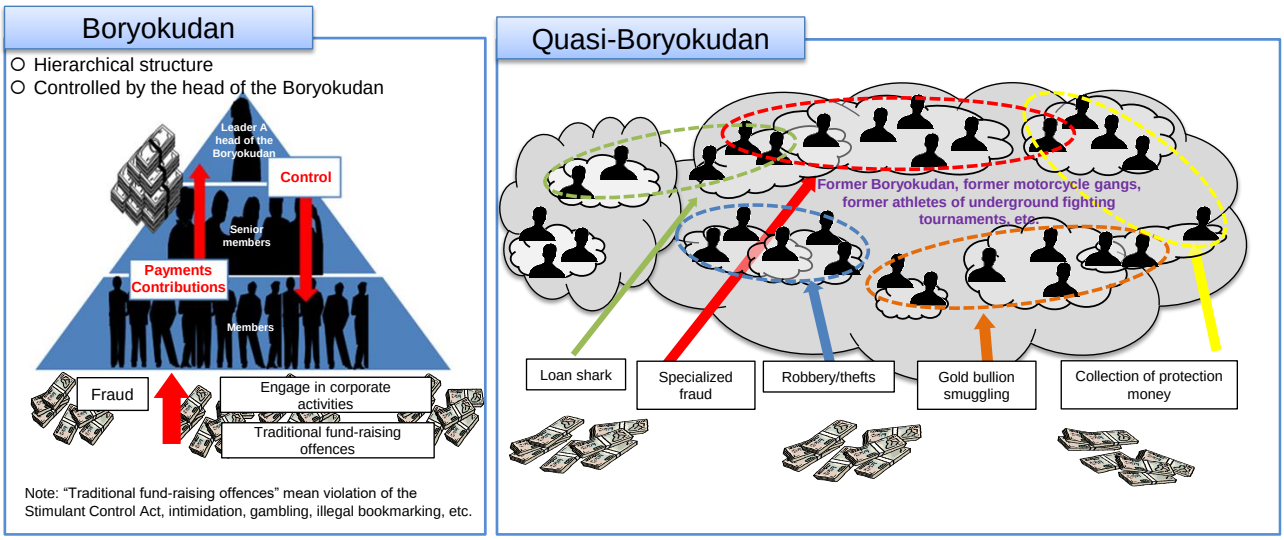
Also, in recent years, groups equivalent to Boryokudan in which persons belonging to the groups perpetrate violent illegal behavior, etc. such as collectively and habitually committing violent acts even though they do not have a clear organizational structure as Boryokudan does (hereinafter referred to as "quasi-Boryokudan") engaging themselves in violent, illegal acts habitually. They have been conducting illegal funding activities, such as fraud (phone scam) and organized theft. These quasi-Boryokudan may have relationships with Boryokudan and contribute some of their abundant funds accumulated through illegal activities to Boryokudan. On the other hand, some cases are also seen where quasi-Boryokudan allocate their funds to operate amusement businesses, etc. or use them to finance other illegal activities to generate income. We can see their situation of trying to maintain and expand the power. Some quasi-Boryokudan members form groups by connecting former members of the motorcycle gang and those who belonged to delinquent groups. In some cases, Boryokudan members skillfully take in quasi-Boryokudan members and form groups like Boryokudan subordinate organizations. Typical examples include former Kanto Rengo Group members and the Chinese Dragon, etc.

---

*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 Anti-social forces include Boryokudan, Boryokudan-affiliated companies, "Sokaiya" racketeers, person(s) engaging in criminal activities under the pretext of social campaigns or political activities, and violent groups/individuals specializing in intellectual crimes.

Table 15 [Figure Showing Structures of Boryokudan and Quasi-Boryokudan]



At the end of 2021, the total number of Boryokudan gangsters was 24,100[*1]including 12,300 Boryokudan members and 11,900 associates[*2]. 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.

(ⅰ) Factors that Increase Risks

(A) Characteristics

Boryokudan have been committing various fund acquisition offenses according to the changing times, such as the trafficking of stimulants, gambling, collection of protection money from restaurants in downtown, intimidation and extortion against companies and administrative agencies, robbery, theft, fraud (phone scam), 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 colluding with persons who cooperate with or assist in the money-making activities[*3], etc. of Boryokudan to conceal their actual state, and their funding activities have become more sophisticated. It is increasingly difficult to define them. Boryokudan 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 used to interfere legal businesses.

Furthermore, quasi-Boryokudan members commit illegal acts, such as fraud (phone scam), organized theft, loansharking, gambling, and extorting money in the name of protection fees and drug trafficking. Besides, it is also recognized that funds are being obtained from amusement businesses, e.g., so-called cabaret clubs and girls' bars, in downtown areas, and other business activities, e.g., restaurants, construction businesses, real estate businesses, and martial arts events. Then, in those business activities, there are cases where unreasonable demands for money are made with the backing of Boryokudan.

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 quasi-Boryokudan collude while evading restrictions under the Anti-Boryokudan Act and the Organized Crime Exclusion Ordinances, etc. to

---

*1 The number of Boryokudan gangsters in this section is an approximate figure.

*2 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.

*3 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.

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

There were 1,769 cleared cases of money laundering from 2019 to 2021, including 180 cases (10.2% of total cases) related to Boryokudan gangsters.

The following cases are the examples of Boryokudan gangsters' involvement in money laundering that occurred in 2021:

- Boryokudan members and persons affiliated with quasi-Boryokudan 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.
- A Boryokudan member used an account in another person's name when receiving criminal proceeds from fraud (phone scam).
- A Boryokudan member made a debtor open an account and used it for receiving payments to a loan shark from other debtors.
- A former Boryokudan member used an account in the name of his acquaintance to steal benefits related to COVID-19.
- 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 2019 to 2022 was 1,402,844, including 176,753 STRs submitted for reasons related to Boryokudan, accounting for 12.6% 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 anti-social forces.

Based on the above guidelines, the Supervision Guidelines established by the Financial Services Agency require deposit-taking institutions, etc. to develop a system to take measures as an organization, establish a centralized management system with a department in charge of handling anti-social forces, conduct appropriate preliminary and subsequent examinations and prevent unreasonable demands made by anti-social forces, etc. in order to eliminate transactions with anti-social forces, and cut off any relationship with anti-social forces.

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 anti-social forces, 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 antisocial forces, such as Boryokudan and quasi-Boryokudan, STRs are submitted.

To thoroughly eliminate Boryokudan from bank loan transactions, in January 2018, the National Police Agency has 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 and other anti-social forces 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 anti-social forces. Since anti-social forces engage in money laundering, transactions with anti-social forces 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 still remain severe, with terrorist attacks occurring in various countries including Europe and the U.S. Also, 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 a third country. 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

After declaring the establishment of a caliphate in 2014, ISIL attracted many foreign fighters who were influenced by its extreme ideology and increased its presence in Iraq and Syria. ISIL is considered to have lost its territory in Iraq and Syria in March 2019 after reducing its territory due to attacks from the military of these countries with the support of other nations.

However, the remaining ISIL forces appear to be still capable of conduction attacks. Its leader, Abu Bakr al-Baghdadi, once again called on his supporters to step up all activities, including attacks and dissemination in his statement issued in September 2019. On October 27, 2019, his death by a US operation was announced. On October 31, ISIL announced that Abu Ibrahim al-Hashimi al-Qurashi had assumed a leadership position in ISIL. On February 3, 2022, he was killed by the U.S. Army, and on March 10 of the same year, ISIL announced that Abu al-Hasan al-Hashimi al-Qurashi had become their new leader.

In retaliation against military intervention in Iraq and Syria, ISIL has continued to conduct terrorist attacks in countries such as the U.S. and European countries that are participating in the Global Coalition to Counter ISIL. For conducting such attacks, ISIL called for fighters to use knives, vehicles, etc. to carry out terrorism when explosives or firearms were unavailable. Even during the spread of COVID-19 that started in 2020, ISIL continued to call for terrorist attacks. Meanwhile, there have been terrorist attacks that are considered to have been influenced by the extremism of ISIL and other groups.

It has been pointed out that some foreign fighters and families in Iraq and Syria, where ISIL has lost the areas under its control, may engage in terrorist attacks in their home countries or in third countries, and that further radicalization may occur in detention facilities and refugee camps.

AQ and associated organizations repeatedly advocate for anti-Americanism and anti-Israelism, and urge members and sympathizers through online bulletins, etc. to carry out terrorist attacks against Western countries.

Also, as AQ-related organizations operating in Africa have been committing terrorism targeting local government organizations and the like, AQ and its related organizations continue to be a threat.

Furthermore, the Taliban seized control of the whole of Afghanistan after the U.S. troops stationed in the country completed its withdrawal at the end of August 2021. The Taliban is said to have close ties with AQ. The security situation in Afghanistan remains unstable, as indicated by a large-scale suicide terrorism attack by ISIL-K[*1] that occurred in August 2021 near the Kabul International Airport in Afghanistan. Thus, there are concerns that Islamic extremist organizations based in the country may become more active.

In Japan, there are people claiming to be in touch with persons affiliated with ISIL and those who express their support for ISIL on the Internet. 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. will commit terrorism in Japan.

---

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

Table 16 [Number of International Terrorism Cases]

Item/year	2018	2019	2020
Number of cases	8,117	8,872	10,172
Number of deaths and injuries	32,952	26,273	29,389

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

Table 17 [Major Terrorism Cases in 2021]

Date	Case
January 21	Case of a suicide terrorist bombing in Bagdad, Iraq
April 23	Case of a terrorist attack with a knife in Rambouillet, France
May 8	Case of a terrorist bombing in Kabul, Afghanistan
July 19	Case of suicide terrorism in Bagdad, Iraq
August 26	Case of a suicide bombing in Kabul, Afghanistan
September 3	Case of a terrorist attack with a knife in Auckland, New Zealand
October 8	Case of a suicide bombing in Kundus, Afghanistan
October 15	Case of a suicide bombing in Kandahar, Afghanistan
October 15	Case of a terrorist attack with a knife in Essex, U.K.

(B) Characteristics

To date no person of Japanese nationality or residency has been included in the list of the targets of asset freeze and other measures pursuant to UNSCR 1267 and succeeding related resolutions and UNSCR 1373 and there has been no terrorist act carried out in Japan by terrorists identified by the United Nations Security Council.

Yet criminals who are wanted internationally for murder, attempted terrorist bombing or other crimes by the International Criminal Police Organization had illegally entered and left Japan repeatedly in the past. This shows that the network of Islamic extremist groups loosely connected through radical beliefs is extending to Japan. In addition, there are people in Japan who support ISIL or sympathize with the group's propaganda. The authorities ascertain that there are people who have made attempts to travel to Syria from Japan in order to join ISIL as fighters.

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

- Terrorist financing may be obtained through taxation imposed by terrorist organizations in transactions conducted in the regions under their control, crimes such as drug smuggling, fraud and 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 international 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 a suspicious transaction 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 the names, aliases and birthdates, concerning persons subject to 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, 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 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 to 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 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 intentional 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.

○ Use of an individual's own savings to recruit and support terrorists (Spain)

In 2016, two individuals were arrested on charges of being the main leaders of a cell in Spain whose aim was to recruit and facilitate FTFs traveling to Syria to join ISIL. One of the two individuals was responsible for approaching and indoctrinating potential terrorists that would subsequently fight in Syria. The second person was in charge of logistics: he maintained Internet fora, bought phone cards and cell phones, and rendered locations secure to hold meetings or buy bus tickets and book hotel rooms. While these two individuals had a criminal history of violent crimes and drug trafficking, the investigators found out that they were investing their own savings and the unemployment benefits received by one of them in order to carry out their activities. They would send small amounts of money, varying from EUR 50 to EUR 150 through Payment Services Companies, to other individuals located across Europe to support the recruitment of new followers for their cause in other foreign countries.

○ Recruitment of IT specialists by terrorist organizations (Indonesia)

In 2012, an IT specialist recruited by a terrorist organization to support terrorist activities through the Internet successfully procured funds for a terrorist organization by breaking into an online-based multi-level marketing (MLM)/investment website. As a result of the hacking activity, the terrorist organization managed to obtain funds. To receive and transfer the funds, the IT specialist used his wife's bank account, borrowed his relative's bank accounts, opened a new account with a false identity, and bought other people's accounts to avoid the tracing of funds. He also kept the value of the transaction in small amounts to avoid suspicion by the bank officials. From the accounts, several cash transactions were carried out to provide funds for a terrorist organization. In the end, the IT specialist was convicted for terrorist involvement by financially supporting a terrorist organization in Indonesia.

---

*1 The Japanese Red Army has caused numerous international terrorism incidents in the past. Seven members still remaining at large are on the Interpol Wanted List, and initiatives continue in efforts to clear cases involving fugitive members and reveal the organization's activities.

○ Middlemen used to distribute funds to promote activities of the terrorist organization (Israel)

In one case, the defendant was asked to deliver money from a terrorist organization to individuals arrested in Israel. These payments amounted to tens of thousands of NIS (ranging from amounts equivalent to 1,000 to 20,000 U.S. dollars). They were paid as a reward to these individuals and their families for committing terrorist acts and continuing to promote the activities of the terrorist organization. The payments were made and transferred to the defendant through unrelated intermediaries who received a commission for their service. On several occasions, the payments were forwarded through the intermediaries, who met in various locations in different cities. In one case, an Israeli citizen met up with a person who entered Israel illegally through the Egyptian border and collected 11,000 U.S. dollars. He later delivered to the defendant in a different city for a commission of 150 U.S. dollars.

For these activities, the defendant was indicted and convicted for several counts, among other things, under the Prohibition on Terror Financing Law. He was sentenced to a 27-month imprisonment and a fine of 5,000 Israeli new shekels (equivalent to approximately 1,250 U.S. dollars).

○ Promotion of crypto-assets to fund terrorism (United States)

In August 2015, an American was sentenced to 11 years in prison to be followed by a lifetime of supervised release. He admitted using Twitter to provide advice and encouragement to ISIL and its supporters. He used Twitter, provided instructions on how to use bitcoin, a crypto-asset, to mask the provision of funds to ISIL, as well as facilitation to ISIL supporters seeking to travel to Syria to fight with ISIL.

Additionally, he admitted that he facilitated travel for a teenager living in the U.S., who traveled to Syria to join ISIL in January 2015.

His twitter account boasted over 4,000 followers and was used as a pro-ISIL platform during the course of over 7,000 posts. Specifically, he used this account to conduct twitter-based conversations on developing financial support for ISIL using online currency, such as bitcoin, and ways to establish a secure donation system or fund for ISIL. For example, the man posted a link to an article he had written entitled “Bitcoin wa’ Sadaqat al-Jihad” (Bitcoin and the Charity of Jihad). The article explained the system of bitcoin and introduced a new tool for keeping the user of bitcoins anonymous.

○ Misuse of Charity for Terrorist-financing (Australia)

In 2015, an Australian bank froze the account of a self-proclaimed humanitarian supporter who belongs to a group called “Street Dawah.” He insisted that he was engaging in humanitarian support for orphans and widows, and stated that he had collected more than 40,000 dollars of donations. He denied that he belonged to ISIL, but he was serving as a recruiter for ISIL. He was also communicating with another Australian radical who was considered to have been involved in a plan for kidnapping and killing citizens in Sydney and also expressing his support for ISIL 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 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 and Control of Crime Proceeds

The Act on Punishment of Organized Crimes and Control of Crime Proceeds 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 file 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 offenses, 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.

○ 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 entities subject to such measures in accordance with the FEFTA. Specifically, as of June 2, 2022, 397 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 2, 2022, the names of 397 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

In December 2013, the Strategy to Make Japan "the Safest Country in the World" was developed with a view to the year 2020, in which the Olympics and Paralympics will be held in Japan, in the Ministerial Meeting Concerning Measures Against Crime chaired by the Prime Minister. Also, in December 2017, the Counter Terrorism Guidance toward the Tokyo 2020 Olympic and Paralympic Games was developed in a meeting of the Headquarters for the Promotion of Measures Against Transnational Organized Crime and Other Relative Issues and International Terrorism, chaired by the Chief Cabinet Secretary.

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] Measures, such as asset freezes, were taken against 5 groups (the New People's Army, al-Shabaab, ISIL

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

Sinai Province, ISIL East Asia Division, and the Maute Group) and 3 groups (the Indian Mujahideen, al-Qa'ida in the Indian Subcontinent, and Neo-JMB) in November 2019 and March 2020, respectively.

While the key to counter-terrorist measure 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

(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 whom asset freezing measures are implemented against pursuant to the United Nations Security Council resolutions (No. 1267 and succeeding resolutions as well as No. 1373), and there have been no terrorist acts carried out in Japan by the terrorists designated by the United Nations Security Council so far.

However, the FATF pointed out in its report[*1] released in 2019 that even when there have not been any cases of terrorist attacks or terrorist financing in a country, that fact does not immediately lead to the conclusion that the risk of terrorist financing is low; the possibility of funds being collected in that country and being remitted 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 avoid their monitoring to be 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.

[Risk of Abuse of Nonprofit Organizations[*2] for TF]

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.

*1 Terrorist Financing Risk Assessment Guidance (July 2019)

*2 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.

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 illegal channels. According to the FATF Recommendations and the Interpretive Notes, etc., nonprofit organizations have the following vulnerabilities to TF:

- Nonprofit organizations have the trust of the general public, can use various sources of funds, and often handle large amounts of cash.
- Some nonprofit organizations conduct activities in regions where terrorist acts occur and their surroundings, and some of them provide systems for financial transactions.
- In some cases, an organization that procures funds for activities and an organization spending such funds are different, which may make the purpose of use of the funds obscure.

When cases in other countries are taken into account, the following threats arise:

- A terrorist organization or a related party establishes a nonprofit organization under the pretext of charity activities, and uses raised funds to support terrorists or their families
- A terrorist organization's related party intervenes in activities of a legitimate nonprofit organization and misuses the nonprofit organization's financial transactions to send funds to terrorist organizations operating in conflict areas, etc.
- Funds obtained through activities of a legitimate nonprofit organization are provided as terrorist funds to another nonprofit organization that has a relationship with a terrorist organization overseas.

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.

As for recent international movements in this context, the "Initiative on Ensuring the Effective Implementation of Countering the Financing of Terrorism Measures While Safeguarding Civic Space ("*shimin-ryoiki-hogo to ryoritsu-shita tero-shikin-kyoyo-taisaku no jikko-kakuho initiative*" (tentative Japanese translation)), was launched by the Global Counterterrorism Forum (GCTF), which is an international framework to combat terrorism. It was established in October 2020 because it was considered important for each national government to consult with a wide range of relevant organizations in order to implement measures for preventing terrorism financing without excessively interfering with the activities of nonprofit organizations. This program held meetings with specialists four times in total to discuss the examples, issues, etc. of different countries.

The establishment and management of nonprofit organizations in Japan are regulated by individual laws such as the Act on Promotion of Specified Non-profit Activities (Act No. 7, 1998, hereinafter referred to as the "APSNPA") and the Act on Authorization of Public Interest Incorporated Associations and Public Interest Incorporated Foundations (Act No. 49, 2006). In addition, although there has been no arrest to date of Japanese nonprofit organizations for being misused for terrorist financing, we need to consider the findings by international organizations when engaging in financial transactions, etc. in light of the position, roles, etc. of Japan as an international financial market. In light of the facts above, each competent administrative authority supervising nonprofit organizations in Japan conducts risk assessment and uses a risk-based approach to monitor nonprofit organizations. The main results of risk assessment of nonprofit organizations conducted by the competent administrative authorities are as follows:

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

Although some CESNAs engage in activities in or around regions facing threats of terrorism or conflict-affected areas, etc. for humanitarian reasons, activities in these areas generally make resource management by CESNA difficult. In these regions, not only do activity areas of CESNAs overlap with those of terrorists but also people in need of support may overlap with those approached by terrorists. This may encourage terrorists to abuse CESNAs for TF.

Some CESNAs can access abundant funds and send the funds overseas to provide support in conflict-affected areas or disaster-affected areas, etc. When CESNAs send the funds, they handle cash intensively, and sometimes transport cash itself. Such funds transfers, in particular, transfers of cash and use of other highly anonymous means of transfer, make tracking of terrorists and their supporters difficult, which encourages abuse of CESNAs.

When CESNAs engage in activities overseas, they often collaborate with local partners, and their activities are supported by a lot of volunteers. Such collaboration with overseas partners and participation of volunteers make identity verification

of those involved in the activities difficult, and may result in the involvement of terrorist organizations and their supporters.

In addition, there are so-called “dormant” CESNAs, as well as those engaging in obscure activities such as CESNAs found to have engaged in no activity or spent no money during the relevant business year in their annual reports. These CESNAs may be abused by terrorist organizations and their supporters.

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.

○ Public Interest Corporations (Cabinet Office)

There are few public interest corporations engaging in activities in or around the regions facing threats of terrorism, and these corporations are at relatively higher risk. Public interest corporations that contract with or assist business operators, etc. for their services in other countries, or those that handle a substantial amount of funds and send money to other countries or handle cash are also at a risk of TF. However, 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 actions 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 actions against such risk. It is important for each public interest corporation 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.

○ Social Welfare Corporations (Ministry of Health, Labour and Welfare)

Overseas activities of social welfare corporations are limited because they are established for the purpose of conducting social welfare business such as management of nursing care homes, etc. Social welfare corporations are required to include provisions concerning overseas activities in their articles of incorporation and obtain the approval of the competent authorities. They are also required to prepare financial statements on overseas activities separately from domestic business.

Social welfare corporations engaging in activities overseas are considered to be at a low risk of abuse for TF because they conduct risk assessment based on the following factors and from the following viewpoints that affect the degree of risk: (i) products and services; (ii) forms of transactions; (iii) countries and regions; and (iv) customer attributes.

○ Medical Corporations (Ministry of Health, Labour and Welfare)

Overseas activities of medical corporations are limited to those related to medical activities. They are required to obtain approvals when conducting overseas activities, and must also report on their activities every year after conducting overseas activities. The MHLW has assessed the risk of medical corporations conducting overseas activities based on the factors that affect the degree of risk, which are (i) products and services, (ii) forms of transactions, (iii) countries and regions and (iv) customer attributes, and considers them as low risk of abuse for TF.

○ Incorporated Educational Institutions (Ministry of Education, Culture, Sports, Science and Technology)

Overseas operations of incorporated educational institutions are limited because they are established for the purpose of setting up and operating private schools. Incorporated educational institutions are required to prepare financial documents and business reports, etc. on their activities, including overseas operations, and make the documents available for access every year. Incorporated educational institutions receiving aid from the competent authorities must also submit financial documents and business reports, etc. to the competent authorities. When engaging in business for profit other than educational and research activities or business associated with educational and research activities, incorporated educational institutions must include them in the articles of endowment and obtain the approval of competent authorities.

Incorporated educational institutions engaging in overseas activities are at a low risk of abuse for TF because they conduct risk assessment based on the following factors and from the following viewpoints that affect the degree of risk: (i) products and services; (ii) forms of transactions; (iii) countries and regions; and (iv) customer attributes.

○ Religious Corporations (Ministry of Education, Culture, Sports, Science and Technology)

Out of the total number of religious corporations (180,544) in Japan, 179,397 corporations (99.4%) are religious corporations engaging in activities in one prefecture, and the competent authority for them is the relevant prefectural

governor. Religious corporations must prepare financial documents, etc. every year. They are also required to grant the right of access to their followers and other interested parties to the documents and submit a copy of the documents to the competent authorities.

Since the legal personality of inactive religious corporations can be abused, the competent authorities collect information on measures against inactive religious corporations actually implemented by appointing a third party to carry out the program for promoting measures against inactive religious corporations, point out the risk of misuse of inactive religious corporations by criminal organizations during the training for persons in charge of administrative work at religious corporations provided by each prefecture to raise awareness, and take other measures to mitigate risks.

There have been no cases where nonprofit organizations in Japan were abused for TF, and it is considered that they are at a low risk of abuse. However, it is still necessary to conduct outreach or monitoring based on risks so that nonprofit organizations will not be abused for TF, etc., considering that some nonprofit organizations engage in activities in countries or regions facing the threats of terrorism, etc. or send money to overseas partners, etc.

(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 than 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 require specified business operators to develop internal control systems for suitable examination and judgment in order to file 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 offenses, 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 revised, 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 the 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 in 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 require specified business operators to conduct enhanced CDD, including verifying the source of wealth, source of funds, customer identification data, etc., when conducting transactions involving the transfer of funds of more than two million yen 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).

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, and 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 require each country to:

- ○ Ensure that business operators conduct customer identification by tracking to a natural person who is a beneficial owner when the customer is a legal person.
- ○ Have mechanisms where beneficial owner of legal persons can be identified, as well as to ensure that competent authorities can obtain or access information on 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 his/her 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, etc. 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 that 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 by registering under the Commercial Registration Act (see Table 18). 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 19). 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[*2]. When establishing a stock company, a beneficial owner must be identified, but such identification is not necessary when establishing a holding company. 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 20).

Table 18 [Number of Corporations by Major Corporate Type in Japan]

Year / Category	2018	2019	2020
Stock company	2,554,582	2,559,561	2,583,472
General partnership companies	3,371	3,343	3,352
Limited partnership companies	14,170	13,540	12,969
Limited liability companies	98,652	113,196	134,142
Others	67,774	68,780	70,436
Total	2,738,549	2,758,420	2,804,371

Note 1: The company sample survey of the National Tax Agency.

*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.

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 19 [Number of Registered Establishments by Each Major Corporate Type]

Year / Category	2019	2020	2021
Stock company	87,871	85,688	95,222
General partnership companies	48	34	16
Limited partnership companies	47	41	33
Limited liability companies	30,566	33,236	37,072
Total	118,532	118,999	132,343

Note: The statistics of the Ministry of Justice.

Table 20 [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 the purpose of 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 mail 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 complex rights/control structure of a legal person, or may substantially control a legal person and its property while obscuring their own 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 in 2021:

- An offender established a shell company, sold embezzled goods by disguising the sale as a legal transaction, and made buyers transfer payments to an account in the name of the shell company.
- An offender made his/her accomplice establish a shell company to receive payments for electronic gift cards obtained through fraud (phone scam) at an account in the name of the shell company.
- An offender sent criminal proceeds obtained through government benefits fraud related to COVID-19 to an account in the name of a company that he/she established by appointing his/her girl/boyfriend as the representative director.
- An offender used an account in the name of a company owned by his/her 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.
- An offender sent criminal proceeds obtained through unlicensed adult-entertainment business to an account in the name of a shell company established by him.

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 are 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.

Of the money laundering offenses cleared from 2019 to 2021, 44 offenses took advantage of dummy or obscure corporations. Similar offenses have been increasing in number in recent years. Of these, 16 offenses took advantage of dummy or obscure corporations in 2021. The number of corporations abused was 23. Looking at the corporations abused by form of legal person, 16 of them are stock companies (including special limited companies), 6 of them are limited liability companies and 1 of them is another form of company.

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 an anti-social force such as Boryokudan.
- ○ A representative director of a company, who is a foreigner, is under the status of residence with restrictions on employment.
- ○ The required license or permit was not obtained for a real estate business or secondhand articles business, etc., and the actual status of business was unclear.
- ○ 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.
- ○ A large amount of transactions, which are suspected to be illegal receipt of government benefits, etc., suddenly occur in a business account that has been inactive for a long time.
- ○ 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.

(ⅲ) Measures to Mitigate Risks

In light of the FATF Recommendations, as well as the adoption of the G8 Action Plan Principles to Prevent the Misuse of Companies and Legal Arrangements 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. that is a legal person. Requires specified business operators performing services to provide companies, etc. with address and facilities for business, means of communication, and address 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 or international terrorist 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 (Act No. 86 of 2005) stipulates 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 FY2014, with approximately 33,000 cases in FY2019, 32,000 cases in FY2020, and 30,000 cases in FY2021.

(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 by form of legal person, existing stock companies are at a 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 difficult 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 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 owner 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, etc. from the prime minister under the Banking Act. As of the end of March 2022, there are 1,344 institutions that 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, 639 agricultural cooperatives and fisheries cooperatives, and 45 credit federations of agricultural cooperatives and credit federations of fisheries cooperatives). Among these institutions, banks held a total deposit balance[*3] of 924.0136 trillion yen for a total of 798,750,000 accounts as of the end of March 2022.

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 that 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, 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 huge number of transactions. As such, it is not easy to find and eliminate 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 countries through Japan's financial institutions as part of their money laundering process.

In addition, the majority of transactions, excluding cash deals, that 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 is higher than that for other business types. The Financial Services Agency is requesting financial institutions that handle deposits to upgrade their AML/CFT systems. The Financial Services Agency evaluates that the level of the overall system is improving. Still, the efforts of some deposit-taking institutions were delayed through the supervision so far. The risk identification or assessment and ongoing CDD of some deposit-taking institutions are insufficient. However, the processes of identifying and assessing the risks

---

*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.

according to the products and services handled, transaction types, countries/regions related to transactions, customer attributes, etc. and reflecting the results of such assessment have started to spread among deposit-taking institutions, which has improved the analysis details in the documents prepared by specified business operators. In order for deposit-taking institutions to implement ongoing CDD, which is important as risk mitigation measure, deposit-taking institutions have established a policy on ongoing CDD including the scope and frequency of investigation, and have started review it timely and periodically in accordance with risk of customers, for the renewal of customer risk assessment. Although it seems that efforts to carry out ongoing CDD have been made, the Financial Services Agency believes that deposit-taking institutions need to continue to strengthen their efforts for renewing their customer risk assessments.

[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-asset exchange service provider made illegal remittances to a bank account opened at a bank by the crypto-asset 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-asset exchange service provider was 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 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 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. fraud (phone scam), 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 names, and accounts illegally opened in the name of shell companies, etc. to deposit criminal proceeds

*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.

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 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 third parties or fictitious persons being used for fraud (phone scam) 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 fraud (phone scam) or cross-border money laundering offences.

In this way, accounts opened under fictitious names or in the names of others are obtained through illegal trading and misused to receive criminal proceeds in fraud (phone scam), loan-shark cases, etc. Proceeds are transferred using such accounts.

Police are strengthening their investigations into violations of the Act on Prevention of Transfer of Criminal Proceeds related to illegal transfer of deposit/savings passbooks and cash cards, including the following case, to be specific.

○ Hundreds of passbooks were seized from the criminal base of a foreigner visiting Japan, who was arrested for illegally soliciting the transfer of accounts through social media, such as buying bank accounts, passbooks, cards, etc.

Many such cases have been cleared. Table 21 shows the number of cleared cases of violating the Act on Prevention of Transfer of Criminal Proceeds as statistics on account transfers etc. Considering these various cases, 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. Furthermore, looking at the number of cleared cases by nationality, Japanese is the highest, followed by Vietnamese and Chinese. Compared to the number of foreign residents in Japan, the cleared cases of account transfer offenses involving foreigners are conspicuous.

In addition, the police are also taking the initiative to crack down account fraud, in which an offender falsely represents the location of a postal receiving service provider as their address when opening an account (account fraud) to obtain deposit/savings passbooks from deposit-taking institutions or receive a passbook knowing that it was obtained illegally. (see Table 22).

Table 21 [Number of Cleared Cases of Violating the Act on Prevention of Transfer of Criminal Proceeds]

Category \ Year	2019	2020	2021
Transfer of deposit/savings passbook, etc.	2,479	2,539	2,446
Transfer of deposit/savings passbook, etc. (business)	44	18	27
Solicitation for transfer of deposit/savings passbooks, etc.	27	32	11
Transfer of exchange transaction cards, etc.	27	35	26
Transfer of information for crypto-assets exchange	0	6	23
Others	0	4	2
Total	2,577	2,634	2,535

Table 22 [Number of Cleared Cases of Account Fraud etc.]

Category \ Year	2019	2020	2021
Account fraud	919	696	710

Transfer of stolen goods	6	7	1
Total	925	703	711

Note: Based on reports on crimes which promote fraud (phone scam), from prefectural police to the National Police Agency.

(b) Deposit transactions

a. Current situation

With the spread of ATMs in convenience stores, 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 fraud (phone scam) cases, deposit transactions are actually misused for money laundering. For example, a crime group made victims, including elderly people, transfer money to the savings account of a third party used by the crime group to withdraw money or transfer money to other 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 other persons' names.
- An offender deposited a large amount of stolen coins into another person's account at an ATM operated by a financial institution and then withdrew it in bills at another ATM.
- A Vietnamese offender transferred proceeds from underground banking into the account of a relative who had become naturalized as Japanese and has a Japanese name.
- An offender deposited cash 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 have 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 another party can ensure anonymity.

The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct verifications 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 received criminal proceeds from fraud (phone scam) by transfer to an account in the name of a shell company that had been illegally opened.
- An offender received money for illegal cross-border remittances requested by clients at an account he bought from a Vietnamese national who has returned to Vietnam.
- An offender sold fake brand goods by cash on delivery, and had a courier company transfer payments from customers to an account in another person's name.
- An offender instructed customers to transfer payments for stimulants or payments to loan sharks to an account in another person's name.
- An offender logged into other persons' online brokerage accounts with illegally obtained account information and transferred the deposits in the accounts to a borrowed account.
- 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.

(d) Safe-deposit box

a. Current situation

A safe-deposit box is a lease of depository. Anyone can operate safe-deposit box businesses, but the most popular operator is deposit-taking institutions, such as banks. They lease their depositories in their premises for 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 physically 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 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 other people's names or fictitious 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 settlement 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 (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 another 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).

(ⅱ) Trends of STRs

The number of STRs submitted by deposit-taking institutions was 1,120,882 between 2019 and 2021, accounting for 79.9% of total reports.

The Financial Services Agency revised the List of Reference Cases of Suspicious Transactions[*1] for deposit-taking institutions by adding reference cases that focus on abnormal transactions specific to Internet-based transactions and financing of terrorism, and released it in April 2019.

Among cases as examples in the List of Reference Cases of Suspicious Transactions, the major ones by number of reports are as follows.

- Unusual transactions or transactions related to customers who show unusual behavior or movements, based on the knowledge and experience of staff (247,022 reports, 22.0%)
- Transactions related to Boryokudan gangsters or their related parties (143,002 reports, 12.8%)
- Transactions involving an account at which frequent remittances from many people are received. In particular, large amounts of remittances or withdrawals from the account immediately after receiving remittances. (86,993 reports, 7.8%)
- Transactions involving large, economically unreasonable amounts of remittances from foreign countries (70,672 reports, 6.3%)
- Transactions involving an inactive account at which a sudden large amounts of deposit transactions are made (67,759 reports, 6.1%)

---

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

- Transactions involving deposits or withdrawals (including trade of securities, remittance, and currency exchange; hereinafter, the same applies) using large amounts in cash or checks. In particular, high-value transactions that were disproportionate to the customer's income or assets, or transactions in which deposits or withdrawals dare to be made in cash even though use of a remittance or cashier's check is considered to be more reasonable (67,729 reports, 6.0%)
- Transactions involving an account to or from which large amounts of deposits and withdrawals are made frequently (42,737 reports, 3.8%)
- Transactions conducted in an unusual manner and with an unusual frequency in light of the purpose of transactions and the occupation or the contents of business that were verified at the time of opening the account. (41,304 reports, 3.7%)
- Transactions involving large amounts of remittances to other countries for economically unreasonable purposes (38,270 reports, 3.4%)

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.

(iii) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds require specified business operators to verify identity and other information in order to implement AML/CFT, and each relevant law and regulation has provisions concerning measures to reduce the degree of risk. The relevant laws and regulations include the following:

- Banking Act

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

(B) Measures by competent authorities

To promote AML/CFT, it is important that specified business operators implement required measures appropriately. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or providing lectures and training, 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 Combating 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 Combating the Financing of Terrorism"	https://www.fsa.go.jp/news/r4/202208_amlcft_faq/202208_amlcft_faq.pdf (Financial Services Agency)
Comprehensive Guidelines for Supervision for Major Banks, etc.	https://www.fsa.go.jp/common/law/guide/city.pdf (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.pdf (Financial Services Agency)
Comprehensive Guidelines for Supervision for Agricultural Cooperative Credit Business	https://www.maff.go.jp/j/keiei/sosiki/kyosoka/k_sido/attach/pdf/index-22.pdf (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/attach/pdf/index-3.pdf (Fisheries Agency)

[Examples of Initiatives Taken by Competent Authorities in 2021]

<Financial Services Agency>

- Revised the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (February 2021)
- 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 in collaboration with the Financial Services Agency (600 cases) (March 2021)
- Requested each financial institution to develop a system by the end of March 2024 in collaboration with the Financial Services Agency (April 2021)
- Amended the "Comprehensive Guidelines for Supervision for Agricultural Cooperative Credit Business," etc. (August 2021)
- Exchanged opinions on each service with persons in charge at all prefectural governments, regional agricultural administration offices, and industry associations, etc.

(C) Measures by industry associations and business operator

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.

(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 to 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

*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.

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 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 2020 involved money transfer to third-party accounts. There were more than a dozen accounts under the names of other people 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 in other people' names are the main criminal infrastructure of ML/TF, among others. Deposit-taking institutions who 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 or fictitious names, borrowed names, and false names (including suspected ones)
- Transactions made by numerous people
- Frequent transactions
- Transactions involving large amounts of remittances and deposits or withdrawals
- Transactions where sudden large deposits and withdrawals are made in accounts that normally do not move funds
- Transactions involving remittances, deposits, and withdrawals performed in an unusual 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 Banks, etc. on Transaction Monitoring, etc.]

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

It is pointed out that banks, etc. not implementing appropriate measures are generally at a risk of ML and other offences.

Based on these facts, banks are specifically considering cooperation for transaction filtering and monitoring, which are the critical operations of for AML/CFT, to make AML/CFT more effective and efficient.

The Act to Partially Amend the Payment Services Act and Other Related Acts to Establish a Stable and Efficient Payment Services System (Act No. 61 of 2022) established and promulgated in June 2022 stipulates that regarding the funds transfer transaction performed for deposit-taking institutions, etc., a system related to "funds transfer transaction analysis service provider" shall be established for banks to cooperate in conducting:

- 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 to deposit-taking institutions, etc.)

and a licensing system shall be introduced to allow the Financial Services Agency, etc. to inspect and supervise "funds transfer transaction analysis service provider".

(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 the characteristics. Insurance companies etc. provide some products that have cash accumulation features. Unlike insurance products that provide benefit based on future accidents, some products with cash accumulation features provide benefit 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 cancelled 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 2021, there were 94 insurance companies, etc. that 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 cancelled the insurance and received a refund soon afterwards (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 another person’s name.

(ⅱ) Trends of STRs

The number of STRs submitted by insurance companies, etc. between 2019 to 2021 was 8,969 (7,353 reports for life insurance, 1,568 reports for non-life insurance, and 48 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 April 2019.

Among the cases listed as examples in the List of Reference Cases of Suspicious Transactions, the main ones according to the number of reports are as follows:

- ○ Life insurance
  - • Transactions related to Boryokudan gangsters or their related parties (5,963 reports, 81.1%)
- ○ Non-life insurance
  - • Transactions related to Boryokudan gangsters or their related parties (557 reports, 35.5%)

---

*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-claims/short-term insurance business operators), and item 20 (mutual aid federation of fishery industry cooperative associations) of the Act on Prevention of Transfer of Criminal Proceeds.

- Unusual transactions or transactions related to customers who show unusual behavior or movements based on the knowledge and experience of staff (98 reports, 6.3%)
- Transactions related to an insurance agreement that is suspected to have been executed in a fictitious or borrowed name (59 reports, 3.8%)

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information to implement AML/CFT. In addition, each relevant law and regulation stipulates measures to reduce the degree of risk. The relevant laws and regulations include the following:

○ 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 Combating 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 Combating the Financing of Terrorism"	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.pdf (Financial Services Agency)
Guidelines for Supervision for Small-Amount and Short-Term Insurance Companies	https://www.fsa.go.jp/common/law/guide/syougaku.pdf (Financial Services Agency)
Comprehensive Guidelines for Supervision for Authorized Specified Insurers	https://www.fsa.go.jp/common/law/guide/ninka_a.pdf (Financial Services Agency)
Comprehensive Guidelines for Supervision for Agricultural Cooperative Mutual Aid Business	https://www.maff.go.jp/j/keiei/sosiki/kyosoka/k_sido/index.html#sinyou_kantoku (Ministry of Agriculture, Forestry and Fisheries)
Comprehensive Guidelines for Supervision for Fishery Cooperative Mutual Aid Business of Fishery Cooperative	https://www.jfa.maff.go.jp/j/keiei/gyokyou/sisin/ (Fisheries Agency)

[Examples of Initiatives Taken by Competent Authorities in 2021]

<Financial Services Agency>

- Revised the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (February 2021)
- 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 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 in collaboration with the Financial Services Agency. (1 case) (March 2021)
- Requested competent associations engaging in mutual aid business to develop a system by the end of March 2024 (April 2021)
- Amended the "Comprehensive Guidelines for Supervision for Agricultural Cooperative Mutual Aid Business," etc. (August 2021)
- 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.

(C) Measures by industry associations and business operator

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. themselves 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 trainings, conduct internal audits, screen out transactions that are considered to be high risk, and adopt enhanced monitoring of high-risk transactions.

[Examples of Initiatives Taken by Industry Associations in 2021]

- Based on the 2021 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)
- Established manuals such as "Paperwork for Fishery Cooperative Mutual Aid "Verifying Identity, etc." (verification of identity and other information under the Act on Prevention of Transfer of Criminal Proceeds)" and "Risk Assessment Report for Transactions in Fishery Cooperative Association" (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 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)
- Ensured that the prescribed identity verification is conducted, and the purpose and route of participation is confirmed when persons other than partners (who are limited to friends and acquaintances of partners or officers and employees under the internal regulations) apply for a mutual aid contract (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 were 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 exploited 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, etc. to another. Insurance companies, etc. taking ineffective risk-mitigating measures corresponding to their risks may face 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 or fictitious names, borrowed names, and false names (including suspicious ones).
- Transactions in which an insurance premium is paid when a contract is concluded and the contract is canceled soon afterwards.

(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 2022, there were 5,159 financial instruments 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 34.

Upon surveying the transactions of stocks and products for investment in Japan, the total transaction volume of stocks listed on the Tokyo Stock Exchange, Inc. (First and Second Sections) was about 773.7594 trillion yen in 2021 (see Table 23).

For commodity derivative transactions, the trading volumes were about 4.03 million sheets[*2] at the Tokyo Commodity Exchange and about 670,000 sheets in 2021 at the Dojima Commodity Exchange.

Investment has different characteristics to deposit/savings; customers risk losing principal when the value 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, etc., 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 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 anti-social forces. In non-face-to-face transactions, there is a risk of dealing with a fictitious person or a person impersonating another person.

Table 23 [Transaction Volume of Stocks]

Year / Category	2019	2020	2021
First Section, TSE	598,213,662	671,671,658	765,249,832
Second Section, TSE	6,188,491	10,657,529	8,509,579
Total	604,402,153	682,329,187	773,759,411

Note 1: Data from the Tokyo Stock Exchange
2: The unit is in million yen.

---

*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 business for foreign investors, etc.) and persons listed in item 33 of the same paragraph (commodity derivatives business operators).

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

(B) Typologies

The following cases are common examples of products and services dealt with by financial instruments business 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 false 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 instruments business operators, etc. and commodity derivatives business operators between 2019 and 2021 were 54,767 and 964, respectively.

The Financial Services Agency, Ministry of Agriculture, Forestry and Fisheries, and Ministry of Economy, Trade and Industry revised the List of Reference Cases of Suspicious Transactions for financial instruments business operators and commodity derivatives business 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 cases as examples in the List of Reference Cases of Suspicious Transactions, the main ones according to the number of reports are as follows.

○ Financial instruments business operators

- Tradings of stocks, bonds, and investments in investment trusts, etc., using accounts suspected to be opened by a fictitious person or in another person's name (13,760 reports, 25.1%)

○ Commodity derivatives business operators

- Transactions in which it was suspected that the customer was using a fictitious or other person's name (652 reports, 67.6%)

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information to implement AML/CFT. In addition, each relevant law and regulation stipulates measures to reduce the degree of risk.

○ 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 Combating 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	https://www.fsa.go.jp/news/r4/202208_amlcft_faq/202208_amlcft_faq.pdf (Financial Services Agency)

Laundering and Combating the Financing of Terrorism”	
Comprehensive Guidelines for Supervision for Financial Instruments Business Operators, etc.	https://www.fsa.go.jp/common/law/guide/kinyushohin.pdf (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 Combating the Financing of Terrorism in the Commodity Derivatives Business	https://www.maff.go.jp/j/shokusan/syoutori/dealing/attach/pdf/money-5.pdf (Ministry of Agriculture, Forestry and Fisheries) https://www.meti.go.jp/policy/commerce/f00/211019amlcft_guideline.pdf (Ministry of Economy, Trade and Industry)
Points to consider for supervision of specified joint real estate enterprises	https://www.mlit.go.jp/common/001390608.pdf (Ministry of Land, Infrastructure, Transport and Tourism)

[Examples of Initiatives Taken by Competent Authorities in 2021]

<Financial Services Agency>

- Revised the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism.” (February 2021)
- 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>

- Amended “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Commodity Derivatives Business” (October 2021)
- Announced the deadline for establishing a system for AML/CFT to members through the industry association Commodity Futures Association of Japan (December 2021)

<Ministry of Land, Infrastructure, Transport and Tourism>

- Issued orders for submission of reports on the development of systems including the facts about transactions and analysis of differences between the facts and the guidelines in collaboration with the Financial Services Agency (74 cases) (March 2021)

(C) Measures by industry associations and business operator

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 2021]

- Issued notices to members regarding policies on measures to take when persons subject to economic sanctions, etc. are designated by a resolution of the United Nations Security Council, such as preparation of a list of foreign customers in alphabetical characters, etc. by each company, and verification of information without delay when information on persons subject to asset freezing is obtained. (December 2021, Japan Securities Dealers Association)
- Conducted a survey 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, and provided the members with information on the results, etc. to raise awareness. (Japan Investment Advisers Association)
- Persons in charge at the secretariat of the associations provided training under the theme "Initiatives by members to implement AML/CFT, etc. (overview of results of questionnaires collected)" (Japan Securities Dealers Association, Type II Financial Instruments Firms Association and 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, investment 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 and 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 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 money laundering, etc., 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 specified 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 specified joint real estate ventures, which comes from distributing profits arising from the execution of a joint real estate venture 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 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 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 2022, 91 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 (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 criminal proceeds. Therefore, it is necessary for trust companies to conduct verification and risk assessment procedures sufficiently not only for settlors but also for beneficiaries as a trustee. For this reason, some trust companies implement measures according to the risks for their beneficiaries, but each trust company takes different measures. Therefore, trust companies need to conduct risk assessments and CDD based on the above-mentioned characteristics.

(ⅱ) Trends of STRs

There were 56 STRs[*2] related to trusts from 2019 to 2021. 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 related to Boryokudan gangsters or their related parties (26 reports, 46.4%)
- Unusual transactions or transactions related to customers who show Unusual behavior or movements based on the knowledge and experience of staff (9 report, 16.1%)

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information in order to implement AML/CFT, and each relevant law and regulation has provisions concerning measures to reduce the degree of risk. The relevant laws and regulations include the following:

- Trust Business Act and Act on Engagement in Trust Business Activities by Financial Institutions

  Stipulate that the Financial Services Agency may require trust companies and financial institutions conducting trust business to report to the Agency as necessary in cases where management systems experience some problems when conducting identify verifications at the time of transactions. Furthermore, if the Agency determines that there are serious problems, it may issue an order for business improvement, etc.

(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

---

*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.

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 Combating 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 Combating the Financing of Terrorism"	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/shintaku.pdf (Financial Services Agency)

[Examples of Initiatives Taken by Competent Authorities in 2021]

<Financial Services Agency>

- Revised the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (February 2021)
- 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 operator

Industry associations support the AML/CFT measures taken by each trust company by providing trainings 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.

(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 on 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 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 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 2022, there were 1,580 registered business operators, while the outstanding balance of loans was 35.1007 trillion yen at the end of March 2022.

(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 another person's driver's license to open a bank account in the name of that person 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 78,013 between 2019 and 2021.

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 April 2019.

Among cases listed as examples in the List of Reference Cases of Suspicious Transactions, the major ones by number of reports are as follows.

- Unusual transactions or transactions related to customers who show unusual behavior or movements, based on the knowledge and experience of staff (23,524 reports, 30.2%)
- Deposits or withdrawals using accounts suspected to be opened by a fictitious or borrowed name (22,610 reports, 29.0%)

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information in order to implement AML/CFT, and each relevant law and regulation has provisions concerning measures to reduce the degree of risk. The relevant laws and regulations include the following:

- 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.

---

*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.

(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 Combating 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 Combating the Financing of Terrorism"	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.pdf (Financial Services Agency)

[Examples of Initiatives Taken by Competent Authorities in 2021]

<Financial Services Agency>

- Revised the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (February 2021)
- 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 operator

Industry associations have developed self-regulating rules that require 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, file STRs when necessary, and prevent damage caused by anti-social forces.

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.

(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 has 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 is 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 2022, there were 83 registered business operators. There were 1,006.7 million remittances totaling 4.2545 trillion yen in fiscal 2020. 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 24).

Table 24 [Trends in Funds Transfer Service Business]

Category \ Year		2018	2019	2020
Number of remittances per year		126,199,274	480,687,760	1,006,699,286
Break down	Domestic	-	430,991,457	936,265,711
	Cross-border	-	49,696,303	70,433,575
Transaction volume per year (million yen)		1,346,370	2,348,439	4,254,499
Break down	Domestic	-	1,220,599	2,854,538
	Cross-border	-	1,127,837	1,399,956
Number of registered funds transfer service providers		64	75	80

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 branch office of a funds transfer service provider and the recipient receives cash at another branch 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, 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.

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 service providers 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

*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.

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, 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. Newly Founded by Competent Authorities]

- 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 identify 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 the fact that its services were contracted out to a sub-contractor and sub-sub-contractor 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 another person'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.
- ○ A person who was leasing a room in a building received proceeds from gambling played in the room in the name of rents 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 services of 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 transfer involving Internet banking to another account and then conducted 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 20,452 between 2019 and 2021.

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 April 2019.

---

*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.

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 having unusual characteristics or conducted at an unusual frequency considering the purpose of the transactions, occupation or business of the client, etc. (3,468 reports, 17.0%)
- ○ Transactions related to Boryokudan gangsters or their related parties (2,352 reports, 11.5%)
- ○ Transactions using accounts that frequently receive remittances from many persons. In particular, cases where an account received a remittance, and then a large amount of money was transferred or withdrawn from the account immediately after receiving the remittance (1,391 reports, 6.8%)
- ○ Transactions related to an account in which frequent remittances are made to many people, especially in the case where large amounts of deposits are made immediately before the remittances (1,200 report, 5.9%)
- ○ Transactions involving an inactive account in which a sudden large amount of deposits and withdrawals occur (910 report, 4.4%)

On top of that, funds transfer service providers made some STRs about Money Mules in recent years. In the STRs, typically, a funds transfer services provider asked a customer the purpose of remittance and found out that he had applied for a job offer on a foreign website and had received money and instructions to forward the money to a foreign country.

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information in order to implement AML/CFT, and each relevant law and regulation has provisions concerning measures to reduce the degree of risk. The relevant laws and regulations include the following:

- ○ Payment Services Act

  Stipulates that the competent authorities have the right to collect business reports from, conduct on-site inspection at 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 Combating 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 Combating the Financing of Terrorism"	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 2021]

<Financial Services Agency>

- Revised the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (February 2021)

- 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 operator

Industry association support AML/CFT measures taken by funds transfer service providers through developing rules for self-regulation and providing training, etc. and created Q&As or other materials regarding the Act on Prevention of Transfer of Criminal Proceeds, etc.

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, etc., established rules and manuals, and screen out transactions that are likely to have higher risks, and adopt enhanced monitoring for transactions with higher risks.

[Examples of Initiatives Taken by Specified Business Operators in 2021]

- Made efforts to strengthen agent management by examining the knowledge of persons in charge of compliance at agencies through interviews upon execution of an agency contract, including AML/CFT measures peculiar to Japan and measures necessary to prevent fraud in agent management programs and audit categories for agencies, and by substantially increasing the number of agencies audited, etc.

(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 exchange transactions.

Actually, there have been cases where criminal proceeds were transferred overseas through funds transfer services by using third parties who were not involved in predicate offenses or by using another 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.

In light of the fact that both the number of remittances per year and the amount handled per year by funds transfer service providers are increasing and the fact that there is an ongoing discussion as to whether the payment of wages to accounts at funds transfer service providers should be allowed or their participation in the *zengin* system (all-bank data telecommunications system) should be allowed, 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 are 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, 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) Crypto-assets Dealt with by Crypto-assets Exchange Service Providers

(ⅰ) Factors that Increase Risks

(A) Characteristics

In Japan, 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 and assets in currency) 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 minister based on the Payment Services Act. As of the end of June 2022, there are 31 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 2021 was a record high of 12,209 cases, loss from ransomware increased, and information leaks caused by illegal access and cyber-attacks by cyber-attack groups supported by national governments occurred.

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. 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 identify the principal, 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. Crypto-assets exchange service providers are expected to establish crypto ATMs or increase the number of units in anticipation of the increase in demand. However, since there are cases in overseas which drug traffickers convert criminal proceeds derived from drug trafficking into bitcoins via crypto ATMs using forged identification documents, it is necessary to watch how such ATMs are actually being used.

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

- There was a case where abnormal crypto-asset transactions were not detected because the effectiveness of transaction monitoring scenarios had not been examined, which resulted in overlooking the implementation of a scenario with specifications that differed from the development requirements.
- There is strong suspicion that business operators engaging in business related to crypto-assets in Japan have been targeted for several years by a cyber-attack group called “Lazarus” in which North Korea is suspected to be involved, considering that the group committed cyber-attacks against crypto-asset exchanges in Japan. These cyber-attack groups disturb blockchain transaction history by using technology called “mixer” when moving stolen crypto-assets to make asset tracing difficult. Authorities in Europe and the U.S. have imposed economic sanctions on mixing services.

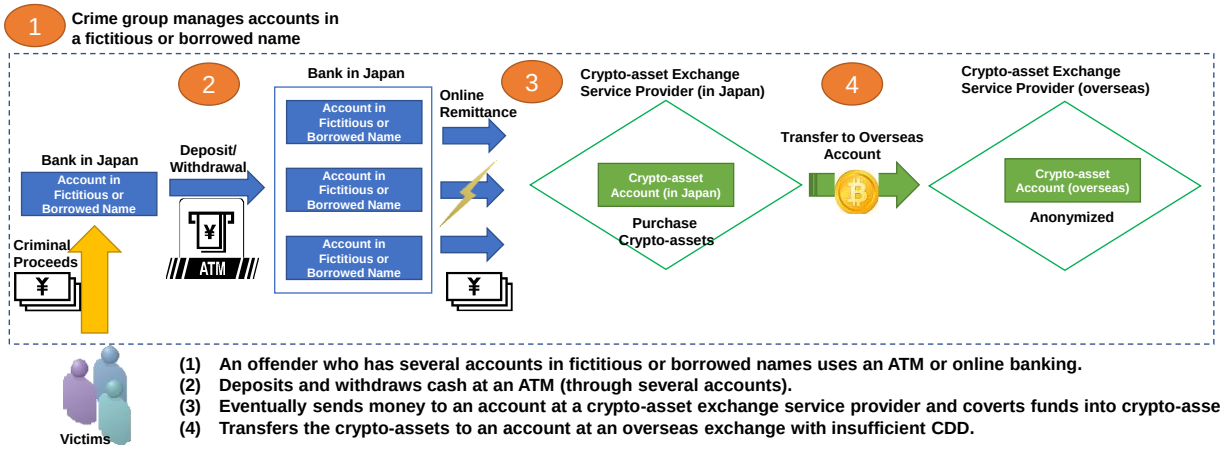
(B) Typologies

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

- An offender purchased crypto-assets by using illegally obtained account information or credit card information belonging to others, exchanged them for Japanese yen through overseas exchange websites, and transferred the funds to an account in another person’s name.

- 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 currencies into cash by transferring the currencies to a crypto address managed by the offender and returning almost the same amount of crypto-assets to the crypto address of the company.

Table 25 [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 another person.

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 2019 and 2021 was 27,559.

The Financial Services Agency created a List of Reference Cases of Suspicious Transactions that includes cases pertaining to transactions on the block chain and the use of anonymization technologies. It was released in April 2019.

Among cases listed as examples in the List of Reference Cases of Suspicious Transactions, the main ones according to the number of reports are shown below.

- Unusual transactions or transactions related to customers who show unusual behavior or movements based on the knowledge and experience of staff (3,102 reports, 11.3%)

○ Transactions conducted frequently in a short period and which involve the sale and purchase of a large amount of crypto-assets in cash, including transactions of an amount slightly less than the threshold (2,527 reports, 9.2%)

○ Deposits and withdrawals of money or crypto-assets, buying and selling of crypto-assets, and exchange with other crypto-assets, using accounts suspected to be opened by a fictitious or borrowed name (2,457 reports, 8.9%)

○ Transactions involving an inactive account in which deposits and withdrawals of funds or crypto-assets in large amounts occur all of a sudden (1,308 reports, 4.7%)

The details of transactions that are suspected to be made with fictitious or borrowed names are as follows:

○ Headshots attached to the principal identification documents of several users with different names and dates of birth were identical

○ More than one 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

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information in order to implement AML/CFT, and each relevant law and regulation has provisions concerning measures to reduce the degree of risk. The relevant laws and regulations include the following:

○ Payment Services Act

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

Stipulates that crypto-assets exchange service providers are required to submit business reports.

(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 Combating 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 Combating the Financing of Terrorism"	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 2021]

<Financial Services Agency>

- Revised the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" (February 2021)

- 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 website of the Financial Services Agency 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.
- Issued a "Request regarding the Travel Rule *1 (such as notification of originator and beneficiary information from crypto-asset transactions)" to the Japan Virtual and Crypto Assets Exchange Association. (March 2021)

(C) Measures by industry associations and business operator

The industry associations established self-regulation rules and guidelines based on the Financial Services Agency's "Guidelines for Anti-money Laundering and Combating the Financing of Terrorism," examined the compliance with the laws and regulations as well as self-regulation rules by the members, provided guidance based on the results of the examinations, and raised awareness regarding crimes involving 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 April 2019, 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 2021]

<Industry Association>

- Raised awareness of users on the member website in response to the Financial Services Agency's announcement on international fraud cases, etc. (October 2021, Japan Virtual and Crypto Assets Exchange Association)

<Specified Business Operator>

- Obtained information on beneficiaries and purpose of remittances from customers before processing crypto-assets transfer transactions to conduct transaction filtering and screening.

(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 in another person's name. For this reason, it is considered that crypto-assets are at risk of abuse for ML/TF.

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.

And, 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.

---

*1 The FATF standards amended in June 2016 specify that each country must introduce and implement regulations to require crypto-assets exchange service providers to obtain originator and beneficiary information from crypto-asset transactions, and notify crypto-assets exchange providers used by beneficiaries of such information.

Although deposit-taking institutions have improved their AML/CFT measures, there are cases where persons who intend to commit ML/TF used crypto-asset transactions in addition to products and services handled by deposit-taking institutions by utilizing the fact that not all deposit-taking institutions have sufficient knowledge about crypto-asset transactions. This situation is increasing the degree of risk associated with crypto-assets.

To deal with such 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 that 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-assets 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.

In the report published in June 2022 titled "Targeted Update on Implementation of the FATF Standards on Virtual Assets & Virtual Asset Service Providers," the FATF pointed out the following issues related to crypto-assets:

- The majority of countries and jurisdictions do not comply with the FATF Recommendation for crypto-assets (Recommendation 15). In particular, only a limited number of countries and jurisdictions have established laws to require notification of information from crypto-asset transactions (the so-called "Travel Rule"); and
- As for technical solution development by the private sector, interoperability between solutions is not secured, or specification of solutions is not in compliance with the FATF standards or regulation, etc. of each country and needs to be improved.

The FATF insists that there are solutions that are in compliance with the Travel Rule and strongly encourages each country to introduce the Travel Rule regulation as soon as possible.

In the report, the FATF also insists that it is necessary to continuously monitor the risks related to Decentralized Finance (DeFi), non-fungible tokens (NFTs)[*1], transactions between individuals without intermediaries (transactions using un-hosted wallets), involvement of traditional financial institutions in crypto-asset markets (e.g. credit card payment services using crypto-assets or so-called Stablecoins, inclusion of crypto-assets in financial assets by institutional investors) and other changes in crypto-asset markets, avoidance of sanctions through abuse of crypto-assets and increase in threats of abuse of crypto-assets by ransomware (e.g. use of crypto-assets exchange service providers with insufficient AML/CFT, use of privacy coins or mixing services, etc.).

The FATF will continue to monitor the status of compliance with the FATF standards, including the Travel Rule, and crypto-assets exchange markets, and report on these matters again around June 2023.

Since it is necessary to keep paying attention to changes and the appearance of risks of abuse of crypto-assets as well as to new technologies related to crypto-assets for ML/TF, the Financial Services Agency considers taking action against the risks related to crypto-assets by, for example, publishing the investigative report titled "Research on Technical Risks, etc. in the Trust Chain of Decentralized Finance Systems" by the Digital and Decentralized Finance Policy Study Group, which was established by the Financial Services Agency.

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 Abbreviation of "Non-Fungible Tokens" and means blockchain-based "unforgeable and immutable digital data." These have a function that secures authenticity by adding a unique characteristic and a function that allows tracing of transaction history.

(8) 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 26).

Table 26 [Transactions by Foreign Currency Exchange Operators]

Reporter \ Year		2019				2020				2021			
		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	Major Bank (Note 2)	4	181,410	26,326	145,738	4	37,298	8,962	240,268	4	12,062	6,738	559
	Local Bank	88	183,687	10,554	57,653	81	39,687	3,706	93,392	72	12,560	3,036	242
	Shinkin Bank	110	3,716	326	88,446	85	718	74	102,808	70	534	65	121
	Foreign Bank	24	375	124	328,477	20	181	59	325,817	19	232	97	418
	Other (Note 3)	9	101,683	5,008	49,344	7	22,848	1,406	61,541	6	7,465	726	97
Businesses Other Than Depository Institutions	Funds Transfer Business/ Credit Card Business	15	230,404	14,952	65,065	6	39,767	3,148	79,168	11	19,420	5,096	1,246
	Hotel Business	34	2,813	161	58,883	23	559	39	69,192	19	65	17	261
	Travel Business	26	54,899	2,421	45,937	16	7,404	381	51,436	10	149	64	429
	Secondhand Articles Dealer Business	48	49,297	3,701	75,139	40	16,309	1,773	108,716	36	10,225	1,965	192
	Airport-related Business	6	154,056	5,377	35,283	3	26,592	998	37,511	3	6,339	432	68
	Large-scale Retail Business	2	230	6	25,949	2	54	2	40,373	1	13	0.3	25
	Other	64	109,611	34,756	355,879	60	45,136	20,607	456,563	41	27,500	9,742	499
Total		430	1,072,181	103,712	96,730	346	236,553	41,155	173,977	292	96,564	27,978	290

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: The major banks 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. It is recognized that deposit-taking institutions are downsizing their foreign exchange services. In addition, due to the decrease in the numbers of foreigners visiting Japan and people traveling overseas as a result of the spread of Covid-19, the number of and the amount involved in foreign exchange transactions have been decreasing recently.

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 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 followings are common examples of misusing foreign-currency exchange for money laundering:

- ○ A large amount of foreign currency obtained due to robbery and murder overseas was converted to Japanese yen through a third party.
- ○ 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 2019 and 2021 was 1,165.

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 cases listed as examples in the List of Reference Cases of Suspicious Transactions, the major ones by number of reports are as follows.

- ○ Currency exchange of large amounts of cash or traveler's checks (268 reports, 23.0%)
- ○ Frequent buying and selling of foreign currency or traveler's checks in a short period of time (218 reports, 18.7%)

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information in order to implement AML/CFT, and each relevant law and regulation has provisions concerning measures to reduce the degree of risk. The relevant laws and regulations include the following:

- ○ 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 2021]

<Ministry of Finance>

- Amended the "Foreign Exchange Inspection Guidelines" (July 2021)

- Submitted a document requesting industry associations and major foreign exchange service providers to develop a system set forth in the above guidelines by the end of March 2024 (July 2021)
- Conducted outreach to major foreign exchange service providers regarding amendment of the above guidelines (October 2021)

(C) Measures by industry associations and business operator

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 launder money or finance terrorism.

Actually, 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 names, borrowed names, 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 counterfeit or stolen currency or suspected like that
- ○ Transactions in which it was suspected that the customer was acting on behalf of other people

(9) 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.

By the way, 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 for paying 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 2019 to 2021 was 556, and the numbers of STRs related to the following transactions included in the types of transactions in the "List of Reference Cases of Suspicious Transactions" were the largest:

- ○ Transactions involving Boryokudan members and persons affiliated with Boryokudan (279 reports, 50.2%)
- ○ Transactions under financial leasing contracts under which customers were suspected to have colluded with suppliers to defraud financial leasing operators of payment for properties without actually installing equipment, etc. (so-called "empty lease") (106 reports, 19.1%)

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

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 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 2021]

<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. (10 companies)
- In response to the publication of 2021 NRA-FUR, requested the Japan Leasing Association to announce the publication to member companies, which was achieved by the Association. (December, 2021)
- 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. (December 2021)

(C) Measures by industry associations and business operator

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 Combating the Financing of Terrorism in Financial Leasing Business	https://www.leasing.or.jp/guideline.html (Japan Leasing Association)

[Efforts Made by Industry Associations in 2021]

- Amended the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Financial Leasing Business. (July 2021, 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 names, borrowed names, 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

(10) 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 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, 2021, 252 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 force 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 credit card obtained through fraud was used to purchase high-price products, and the products were sold to a second-hand articles dealer through the use of a false ID.
- 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 sent 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 shipping site's payment system.

(ⅱ) Trends of STRs

The number of STRs submitted by credit card operators was 88,733 between 2019 and 2021.

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 cases listed as examples in the List of Reference Cases of Suspicious Transactions, the major ones by number of reports are as follows.

- Credit card contracts in which it was suspected that the customer used a fictitious or other person's name (25,699 reports, 29.0%)
- Credit card contracts that are suspected to have been executed in a fictitious or borrowed name (21,685 reports, 24.4%)
- Transactions related to Boryokudan gangsters or their related parties (10,277 reports, 11.6%)

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information in order to implement AML/CFT, and each relevant law and regulation has provisions concerning measures to reduce the degree of risk. The relevant laws and regulations include the following:

---

*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).

○ Installment Sales Act

Stipulates that the competent authorities have the right to collect reports from, conduct on-site inspection at 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 Combating 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 2021]

<Ministry of Economy, Trade and Industry>

- Amended the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Credit Card Business." (November 2021)
- Requested credit card operators to establish an AML/CFT system through the Japan Consumer Credit Association. (December 2021)
- Provided specified business operators with training, etc. on AML/CFT in collaboration with the industry associations.

(C) Measures by industry associations and business operator

The industry associations have added provisions concerning verification of identity and other information at the time of transactions and STRs to their self-regulatory rules and requested their members to take appropriate measures. Furthermore, the Japan Consumer Credit Association conducted training for members based on the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in 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 credit information institutions designated by the Minister of Economy, Trade and Industry under the Installment Sales Act about information on credit card members, credit card operators can check the presence of any suspicious points, such as a large number of applications for credit cards made in a short period, and use the results as references when deciding the conclusion, renewal, etc. of contracts. Credit card operators also make their own voluntary efforts. For example, they set a maximum usage amount on each card holder after a strict admission/renewal check, screen out transactions that are considered to be high risk, adopt enhanced monitoring for transactions at high risk, introduce a system to prevent credit cards being used by a person who pretends to be a true card holder in non-face-to-face transactions (i.e. setting a password, etc.), conduct customer identification in face-to-face transactions to prevent credit cards being used by a person who pretends to be a true card holder, and have periodic meetings with law-enforcement authorities.

[Examples of Initiatives Taken by Industry Associations in 2021]

- Provided information, including information on ML, at an information meeting for members in eight areas in Japan. (September to December 2021; Japan Consumer Credit Association)
- Provided members with online lectures on ML. (December 2021; Japan Consumer Credit Association)

(ⅳ) Assessment of Risks

Credit cards allow a holder of criminal proceeds in cash to transform them into different kinds of property. It is also possible to transfer funds by providing a credit card to a third party and making him purchase products. Considering this, it is recognized that credit cards present the risk of misuse for ML/TF.

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 names, 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

(11) 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 owner of real estate by purchasing it under a fictitious or other person'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 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 128,597 brokers as of the end of March 2022. In 2020, the annual amount of sales was about 44 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, was approximately 190,000. Business scale varies significantly across the real estate broker industry. While there are major brokers who handle several thousands of 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 illicit sale of drugs. (case in a foreign country)

(ⅱ) Trends of STRs

The number of STRs submitted by real estate brokers was 17 between 2019 and 2021. Among cases listed as examples in the List of Reference Cases of Suspicious Transactions, the major ones (and the number of reports) are as follows.

- Purchase of building lots or buildings in large amounts of cash (9 reports, 52.9%)
- Unusual transactions or transactions related to customers who show unusual behavior or actions, based on the knowledge and experience of their own employees (3 reports, 17.6%)

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 is 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 person were found to be Boryokudan gangsters as a result of investigation.

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information in order to implement AML/CFT, and each relevant law and regulation has provisions concerning measures to reduce the degree of risk. The relevant laws and regulations include the following:

○ 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

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 2021]

<Ministry of Land, Infrastructure, Transport and Tourism>

- Requested supervisory authorities to enhance supervision of the status of compliance with the obligations under the Act on Prevention of Transfer of Criminal Proceeds, and also conduct on-site inspections.

(C) Measures by industry associations and business operator

Furthermore, the Liaison Council for Preventing Transfer of Criminal Proceeds and Prevention of Damage by Anti-social Forces in Real Estate Business is working to secure effective implementation of the Act on Prevention of Transfer of Criminal Proceeds. For example, this Council arranged an agreement on real estate brokers' developing a management system to prevent transfer of criminal proceed and damage by anti-social forces, and distributes leaflets about announcements and education continuously. 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 cancelled 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 anti-social forces, real estate brokers independently prepare a checklist on the speech and behavioral characteristics of anti-social forces and utilize the checklist for CDD.

[Examples of Initiatives Taken by Industry Associations in 2021]

- Announced the results of the FATF's mutual evaluation of Japan and further promotion of AML to member companies. (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.

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, and real estate brokers 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 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.

(12) 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 the tax system of Japan and that of a foreign country to illegally obtain proceeds. Specifically, offenders can obtain proceeds equal to consumption taxes by purchasing gold bullions 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 2020 administrative year[*2], the number of processed cases (notifications and indictments) of gold smuggling was 20 (90% decrease compared to the previous administrative year), and the value of evaded taxes was about 90 million yen (75% 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 jewelries, payments are usually made with a credit card or by bank transfer, and cash transactions are uncommon. Therefore, from the viewpoint of traceability of funds, the risk of misuse for ML/TF is evaluated as relatively low. On the other hand, there are certain risks for department stores and major jewelers who handle numerous high-priced items. Furthermore, the Ministry evaluates that companies handling precious metals, which often conduct transactions at a scale unsuitable for the company size or transactions with non-residents, have a high risk of misusing them for ML/TF.

(B) Typologies

The following cases are common examples of misusing precious metals and stones for 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 in the name of another person at a jewelry store using cash obtained through theft.
- An offender sold stolen ornaments containing precious stones to a pawnbroker by impersonating another person.

---

*1 Means precious metals set forth in Article 6, paragraph 1, item 10 of the FEFTA.

*2 The period from July 2020 to June 2021.

These transactions were conducted with an increased level of anonymity, by impersonating to another person or falsifying identification data, etc. through the presentation of forged ID 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 that precious metals and stones are misused for money laundering due to their high anonymity and the ease of liquidation and transportation.

(ⅱ) Trends of STRs

The number of STRs submitted by dealers in precious metals and stones was 328 between 2019 and 2021. Among cases listed as examples in the List of Reference Cases of Suspicious Transactions, the major ones by number of reports are as follows.

- The same person/company buying and selling a large amount of precious metals and stones in a short period (141 reports, 43.0%)
- Frequent purchases in small amounts, resulting in a large amount of purchases (47 reports, 14.3%)
- Large purchases not corresponding to the income or assets, etc. of customers (43 reports, 13.1%)

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information in order to implement AML/CFT, and each relevant law and regulation has provisions concerning measures to reduce the degree of risk. The relevant laws and regulations include the following:

- 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 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 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 for Anti-Money Laundering and Combating the Financing of Terrorism in Dealers 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 2021]

<Ministry of Economy, Trade and Industry>

- Provided explanations about compliance with the Act on Prevention of Transfer of Criminal Proceeds, etc. and an executive summary of the Fourth Round of Mutual Evaluation of Japan by the FATF at a seminar held by the Japan Gold Metal Association for its members. (November 2021)

(C) Measures by industry associations and business operator

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, Ministry of Finance and Tokyo Metropolitan Police Department 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 2021]

- Announced the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Dealers in Precious Metals and Stones" to members. (Japan Reuse Affairs Association, Antique Dealers Federation of Tokyo and Nationwide Pawnshop Union Alliance Society)
- Provided information about AML/CFT by organizing workshops for member companies, with employees of the Ministry of Economy, Trade and Industry as lecturers, and explaining the obligations to comply with the Act on Prevention of Transfer of Criminal Proceeds. (November 2021, Japan Gold Metal Association)
- Distributed leaflets and guidebooks containing an overview of the Act on Prevention of Transfer of Criminal Proceeds and obligations of business operators at a jewelry exhibition venue to provide information about AML/CFT and raise awareness. (Japan Jewelry Association)

(ⅳ) Assessment of Risks

Precious stones and metals 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.

Taking into account the crimes committed in relation to gold bullion in recent years, it is believed that the risk in which gold bullion is misused for ML/TF is increasing.

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, and dealers in precious metals and stones 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 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.

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

(ⅰ) Factors that Increase Risks

(A) Characteristics

In postal receiving service business, service providers consent to customers using the service's own 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 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 fraud (phone scam), 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 fraud (phone scam), 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 2019 and 2021. 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' own 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 fraud (phone scam) 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 another persons' name.

(ⅱ) Trends of STRs

The number of STRs from postal receiving service providers between 2019 and 2021 was 6.

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 cases listed as examples in the List of Reference Cases of Suspicious Transactions, the major ones by number of reports are as follows.

- Transactions related to customers who show unnatural behavior or attitude in the process of making contract that was noticed based on the knowledge and experience of staff (3 reports, 50.0%).

There were no STRs submitted in 2021.

There have been STRs on suspected impersonation indicating that applicants could not answer inquiries about basic information, such as their age, and STRs about cases where offenders came to pick up parcels by impersonating a contractor.

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

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 submission of reports or 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. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or holding seminars, etc. for specified business operators.

[Guidelines, etc. Established by Competent Authorities]

Name of Guidelines, etc.	Website's URL, etc.
Guidelines for Anti-Money Laundering and Combating 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 2021]

<Ministry of Economy, Trade and Industry>

- Established the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in Postal Receiving Services." (December 2021)

(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 cancelled 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.

Actually, there are cases where offenders made contract 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 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, and postal receiving service 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 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 of a postal receiving service using multiple companies' names
- Transactions with customers who often receive large amounts of cash

(14) 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 to 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 (phone scam), 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 transaction, 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 2019 and 2021 was none.

(ⅲ) Measures to Mitigate Risks

(A) Statutory measures

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 submission of reports or 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. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or raising specified business operators' awareness.

[Guidelines, etc. Established by Competent Authorities]

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

[Examples of Initiatives Taken by Competent Authorities in 2021]

<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 2021)

- Issued an overview of the Act on Prevention of Transfer of Criminal Proceeds and information that needs be verified at the time of transactions to business operators that had provided notification under the Telecommunications Business Act. (August 2021)

(ⅳ) Assessment of Risks

Recently we have not seen any cleared cases for money laundering involving misuse of a 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, and telephone receiving service providers that are not taking effective mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, which will influence the risk for the industry as a whole.

(15) Telephone 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 2022, there were 884 providers that 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 fraud (phone scam) 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 do not have such facilities or equipment so the latter can use the cloud PBX owned by the former. Fraud (phone scam) cases use the telephone forwarding services of a provider that has purchased telephone lines from another company. This interferes with the investigation of fraud (phone scam) cases because it takes time to verify the person who concluded the contract with the telephone forwarding service provider, who is the end client.

Actually, 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 fraud (phone scam), 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 24 reports in accordance with the Act on Prevention of Transfer of Criminal Proceeds during the period from 2019 to 2021. The details of major violations of obligations discovered as a result of collecting the reports in 2021 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.

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 forwarding services contracted under another person's name were misused for communication with customers.

As the above case shows, telephone forwarding services are misused as 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 fraud (phone scam).

---

*1 Services to enable call functions (such as an internal line, an external line, and call forwarding) through cloud migration of a private branch exchange (PBX) via a designated line or the Internet.

(ⅱ) Trends of STRs

There were 8 STRs from telephone forwarding service providers between 2019 and 2021. 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 involving services that are likely to be used by customers with the intention to disguise the substance of a company, etc., which are suspected of being used for ML/TF during the process of executing a contract (1 report, 12.5%).
- ○ Transactions where the customer is suspected of having entered a contract under a fictitious or other person's name in the process of concluding a contract (1 report, 12.5%).

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

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to verify identity and other information in order to implement AML/CFT, and each relevant law and regulation has provisions concerning measures to reduce the degree of risk. The relevant laws and regulations include the following:

- ○ 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. The competent authorities have been making efforts to ensure that specified business operators carry out such measures by establishing guidelines or raising specified business operators' awareness.

[Guidelines etc. Established by Competent Authorities]

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

[Examples of Initiatives Taken by Competent Authorities in 2021]

<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 2021)
- Issued an overview of the Act on Prevention of Transfer of Criminal Proceeds and information that needs be verified at the time of transactions to business operators that had provided notification under the Telecommunications Business Act. (August 2021)

- Included IP telephone numbers that start with 050, in addition to landline numbers, subject to suspension of use by telecommunications business operators upon abuse for fraud (phone scam). (November 2021)
- Issued improvement orders against four telephone forwarding service providers for violating their obligations to verify identity and other information at the time of transactions in accordance with the Act on Prevention of Transfer of Criminal Proceeds.

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 2021, the Ministry issued a rectification order to 4 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 recurrence.

The police cleared 2 of these cases, in which telephone forwarding service providers failed to comply with improvement orders issued by the Minister of Internal Affairs and Communications for violation of the Act on Prevention of Transfer of Criminal Proceeds (violation of improvement order) in 2021.

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 fraud (phone scam), etc. by giving guidance to them.

Offenders of frauds (phone scam) 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 suspensions request from the Police if those numbers are used for crimes.

Since there were cases where specified IP telephone numbers (IP telephone numbers starting with 050) were abused for fraud (phone scam), 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.

(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 fraud (phone scam), 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 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, and telephone forwarding service providers that are not taking effective 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 frauds (phone scam), 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.

(16) 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 roll of attorneys 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 2022, 42,897 lawyers, 6 Okinawa special members, 455 foreign lawyers, 1,496 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 2022, 22,907 judicial scriveners and 995 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 2022, 50,286 administrative scriveners and 1,000 administrative scrivener corporations are registered.

Certified public accountants shall make it their practice to audit or attest to financial documents. They may also make it their practice to compile financial documents, 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 2022, 33,215 certified public accountants, 2 foreign certified public accountants, and 273 audit firms are registered.

Certified public tax accountants represent clients for filing applications and requests, reporting, preparing statements under laws regarding tax payment to tax agencies, preparing tax forms, and consulting about taxation. Other than that, as incidental business of the mentioned above, they prepare financial forms, keep accounting books on their clients' behalf, 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 2022, 80,163 certified public tax accountants and 4,601 certified public tax accountants' corporations are registered.

As mentioned above, legal/accounting professionals possess expertise regarding law and accounting. They have good social credibility and are involved in a wide range of transactions.

However, for those who attempt ML/TF, legal/accounting professionals are useful because they have indispensable expertise in legal/accounting fields to manage or dispose of property for those purposes. At the same time, they can use their high social credibility to lend the appearance of legitimacy to dubious transactions and asset management activities.

Furthermore, 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:

---

*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.

- 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 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 and 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 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 the submission of reports or 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.

(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 conducted an interview-based survey with large law firms and a follow-up survey regarding answers in annual reports, analyzed the types of high-risk transactions, and summarized the results of the analysis in the "Risk Assessment of Money Laundering in Legal Practice" (hereinafter referred to as the "Legal Practice Risk-NRA-FUR") to promote lawyers' understanding of risks in legal services. 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 JFBA, lawyers should pay attention to the following matters for AML/CFT measures:

- Refer to the Legal Practice Risk-NRA-FUR 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, 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*.

The JFSA requested each Shiho-Shoshi's Association to appoint a person and department in charge of AML/CFT. In addition, the JFSA plans to hold meetings for people in charge at the Shiho-Shoshi's Associations to share information on the results of the FATF Fourth Round of Mutual Evaluation Report of Japan and their impacts on judicial scriveners' services. It will also prepare questions to be included in the "Specified Incident Report" (report on status of compliance with the Act on Prevention of Transfer of Criminal Proceeds, etc.) and information on how to answer the questions, as well as guidelines for anti-money laundering and combating the financing of terrorism in judicial scriveners' services.

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. In addition, JFCAPLSA announced the actual situation related to AML/CFT measures and the importance of such measures to all of its members, as well as the recognized risks related to services of administrative scriveners, etc., through the above website from April 2018 to March 2020.

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 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. In 2021 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.

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 transaction, and create and save confirmation records and the transaction records.
- Refer to the business and the transactions to be provided to the client, identify and assess risks, 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 online 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 accounts' 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.

Actually, there are cases where services of legal/accounting professionals have been misused to disguise concealment of criminal proceeds as legitimate transactions. Considering this, it is recognized that when legal/accounting professionals conduct 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 expertise and valuable social credibility which 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.

[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 cash intensive businesses, often operating 24 hours per day, with 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 weaknesses in staff training and AML/CFT competencies.

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 require casino business operators to verify identity and other information of customers at the time of transactions, prepare and keep identification and transaction records, and submit STRs. The Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds amended by the Order for Enforcement of the IR Development Act (Cabinet Order No.72 of 2019) stipulates that the following transactions are the "specified transactions" including 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 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)

*1 Vulnerabilities of Casinos and Gaming Sector (March 2009)

○ To report to the Casino Regulatory Commission when the total amount involved in a transaction involves receipt or payment of cash exceeds one 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 July 2022, the review standards for disposition of a casino business license, etc. were established, and an environmental arrangement is being made to prevent casinos from being abused by ML.

[Measures for Electronic Payment Instruments, etc. (so-called "Stablecoins" that are expected to be widely used as means of funds transfer and payment) and High-value Electronically Transferable Prepaid Payment Instruments]

1. Electronic Payment Instruments, etc.

(1) Vulnerabilities in Products and Services

Although there is no universally accepted definition for so-called "Stablecoins," in general, a "Stablecoin" means a digital asset that aims to maintain a stable value by being pegged to specific assets and uses distributed ledger technology*1 (or similar technology). It is pointed out that Stablecoins may be used as means of funds transfer and payment in a wide range of areas in the future. Looking at the situations where these Stablecoins were used, in many cases they were used as part of crypto-asset transactions. According to the FATF, etc., these transactions have the following characteristics:

○ Some business operators do not securely protect funds received from customers.

○ Due to the global use of Stablecoins, they are in circulation on permissionless distributed ledgers and are likely to increase P2P transactions*2, which are not subject to regulations, whereby they are at a high risk of ML/TF.

○ The advantages of permissionless distributed ledgers and systems using such ledgers are that they help to eliminate single points of failure*3, etc. On the other hand, they cause problems for AML/CFT because of P2P transactions.

At an international level, measures for so-called global Stablecoins were vigorously discussed at the G20, the Financial Stability Board (FSB), FATF and other international standards-setting bodies, and the FSB published ten recommendations for regulating Stablecoins and other reports based on the policies "to apply the same rules to the same business and same risks." It is emphasized that each country needs to establish rules before global Stablecoin services are provided.

(2) Measures under Laws and Regulations

In light of the above, it was determined that the following measures will be taken: intermediaries for transactions of so-called Stablecoins that are expected to be widely used as means of funds transfer and payment will be designated as Electronic Payment Instrument Exchange Service Providers, etc. under the Payment Services Act, etc. to require them to register as stipulated in each business law; and the Electronic Payment Instrument Exchange Service Providers, etc. will be designated as specified business operators under the Act on Prevention of Transfer of Criminal Proceeds from the viewpoint of preventing their services from being misused for ML/TF. This will require them to assume obligations including the obligations to verify identity and other information at the time of transactions and obligations to submit STRs.

2. High-value Electronically Transferable Prepaid Payment Instruments

(1) Vulnerabilities in Products and Services

Prepaid payment instruments were institutionalized as means of payment to issuers and participating stores, and they were not intended to be used for provision of services such as electronic transfers. However, in recent years, prepaid payment instruments, which can be used to pay for various goods and services at a wide range of stores, emerged on online platforms or as a form of international credit card, etc. Although they do not allow users to claim refunds from issuers, their functions are similar to those of cash. The facts about IC prepaid payment instruments and server prepaid payment instruments (other

*1 Distributed ledgers are generally categorized into permissionless ledgers that allow everyone to participate in the network, and permissioned ledgers that require authorization by administrators to participate in the network.

*2 Means transactions of Stablecoins between individuals without involvement of specified business operators that assume the obligations related to AML/CFT.

*3 Part constituting a system that, if it fails, will stop the entire system.

than paper and magnetic prepaid payment instruments) which form a large percentage of the third-party prepaid payment instruments used in Japan are as follows:

○ Like transportation IC cards, many of them cannot be assigned or transferred electronically. The maximum amount that users can add to them is small, and they are used for small payments (prepaid payment instruments for micropayments).

○ On the other hand, balance-transfer type and number-notification type prepaid payment instruments are provided as electronically assignable and transferable prepaid payment instruments (collectively, "Electronically Transferable Prepaid Payment Instruments"). Electronically Transferable Prepaid Payment Instruments include those that allow users to load a large amount of money onto them (including those with no limit, hereinafter referred to as "High-value Electronically Transferrable Prepaid Payment Instruments").

○ It is thought that only a limited number of users load large amounts or assign large amounts to others by using balance-transfer type prepaid payment instruments. For example, prepaid cards of international brands allow users to load tens of millions of yen.

Since, in principle prepaid payments instruments are non-refundable, issuers of prepaid payment instruments are not required to assume the obligations under the Act on Prevention of Transfer of Criminal Proceeds, including the obligations to verify identity and other information at the time of transactions and obligations to submit STRs, unlike banks and other deposit-taking institutions or funds transfer service providers. Moreover, they are not required to set a maximum amount for each user under the Payment Services Act in effect.

In general, vulnerabilities in AML/CFT are targeted by offenders for abuse of provided products and services for ML/TF. Therefore, it is necessary to take multilateral measures, paying attention to the functions of services provided. There is a belief that the risk of abuse of prepaid payment instruments for ML/TF is small because issuance of refunds is not allowed for prepaid payment instruments, and this does apply to prepaid payment instruments for micropayment widely used in Japan that are not electronically assignable and transferable and allow users to load only a small amount (e.g. transportation IC cards). However, such concept does not apply to other prepaid payment instruments, so action is required based on the risks presented.

[Cases where Prepaid Payment Instruments Were Abused for ML]

○ An offender sold electronic money obtained from fraud through an online intermediary and received payments for the electronic money by transfer to a bank account in another person's name.

○ An offender used an illegally obtained credit card information to load a virtual prepaid card created in another person's name online with electronic money, used it to pay for living expenses, etc. and also sent money to a different virtual prepaid card created in another person's name.

○ An offender increased the balance in an electronic money account registered by disguising him/herself as a fictitious person when receiving payments for illegal videos.

(2) Measures under Laws and Regulations

Based on the above points of view, issuers of prepaid payment instruments that allow high-value electronic transfers (hereinafter referred to as the "High-value Electronically Transferrable Prepaid Payment Instruments") need to take the same actions as those that specified business operators, including banks and other deposit-taking institutions, funds transfer service providers, crypto-assets exchange service providers, and credit card business operators, are required to take under the Act on Prevention of Transfer of Criminal Proceeds to implement AML/CFT.

For this reason, it has been decided that the issuers of the High-value Electronically Transferrable Prepaid Payment Instruments will be added to specified business operators under the Act on Prevention of Transfer of Criminal Proceeds. This will require them to assume obligations such as the obligation to verify identity and other information at the time of transactions and the obligations to submit STRs.

In addition, it has been decided that the Payment Services Act will require issuers of High-value Electronically Transferrable Prepaid Payment Instruments to assume the obligations to submit business implementation plans to enhance monitoring by the authorities.

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, etc.	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 those provide legal persons, etc. with an address, facilities, means of communication for business/management present risks of being misused for ML/TF because such services may create a fictitious or exaggerated appearance of business credibility, business scale, etc. However, once it becomes problematic for those services to disguise the actual status of their legal person etc., it in turn becomes difficult to misuse them for ML/TF.
(vi)	Minimal or no fund-accumulation features	Investment in products or services with no or minimal fund-accumulation features is inefficient for ML/TF.
(vii)	The transaction amount is less than the regulatory threshold	Transactions below the regulatory threshold are inefficient for ML/TF[*1].
(viii)	Customer identification measures are secured by laws, etc.	In some transactions, customers or beneficiaries are verified under laws, etc. or are limited to persons who, conforming with business regulations, obtained a business license from the national government, etc. Thus, customers' identities are clear and fund traceability is secured in such transactions.

*1 In the FATF Recommendations and Interpretative Notes etc., the FATF also sets out transaction amounts that are the thresholds for CDD measures. However, if one transaction above the threshold is divided into several transactions and the amount of each divided transaction falls below the threshold, such an action (structuring) is to avoid regulation, and has a high risk of being misused for ML/TF. The Act on Prevention of Transfer of Criminal Proceeds and the Enforcement Order provide that when specified business operators conduct two or more transactions (receipt or payment of cash, withdrawal of deposit/savings, foreign currency exchange, sales of precious metal, etc.) with the same customer at the same time or continuously, and the transactions obviously represent a divided single transaction, the separate transactions should be regarded as a single transaction.

2. Types of Low-risk Transactions

Specific transactions that have factors to mitigate risks described in 1. above are as follows.

However, even if a transaction falls under a category shown below, if it is a suspicious transaction or one that requires special attention in CDD, it is not recognized as a low-risk transaction[*1]

	Specific Types of Low-risk Transactions		Reasons Listed in 1. Above
1	Certain Transactions in Money Trusts, etc.	Transactions conducted for the purpose of managing assets to be returned to the beneficiaries as set forth in Article 4, paragraph 1, item 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[*2], 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.[*3] 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)

*1 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 require verifications at the time of transactions. However, such transactions are not excluded from specified businesses that require the preparation and retention 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.

*2 In group insurance, the amount that is deducted from the salary of employees is used for premiums.

*3 Financial instruments exchange markets prescribed in Article 2, paragraph 17 of the Financial Instruments and Exchange Act or over-the-counter securities markets prescribed in Article 67, paragraph 2 of the same Act, or foreign markets (only in jurisdictions designated by the Financial Services Agency Commissioner) where sales and purchase of securities equivalent thereto or Foreign Market Transaction of Derivatives prescribed in Article 2, paragraph 23 of the same Act is carried out.

		Individual Credit*1 set forth in Article 4, paragraph 1, item 6, (c) of the Ordinance, etc.	(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 an amount 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)
		Foreign 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 foreign exchange transactions, for which verification of identity and other information of a payer is conducted by a payee in the same manner as specified business operators as set forth in Article 4, paragraph 1, item 7 of the Ordinance	(vii), (viii)
8	Opening a Special Account under the Act on Book-Entry Transfer of Corporate Bonds and Shares	Opening special accounts under the Act on Book-Entry Transfer of Corporate Bonds and Shares as set forth in Article 4, paragraph 1, item 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*2	(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	Transactions in which precious metals, 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)

*1 Individual credit is a type of transaction. When purchasers buy products from sellers, purchasers do not involve cards, etc. Instead, an intermediary provides the amount equivalent to the product price to the seller according to the contract with purchasers and sellers, and purchasers make payment of the price according to a certain fixed method to the intermediary later.

*2 Transactions carried out between 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 use a specified communications method (which means an international communications method used between a specified business operator, the Bank of Japan, and a foreign specified business operator, for which necessary measures are taken to identify the specified business operator, the Bank of Japan, and the foreign specified business operator by the Commissioner of the Financial Services Agency, who communicate with each other through the said communications methods) as a customer, etc. and for which verification is made or settlement is directed through the said specified communications method. SWIFT (Society for Worldwide Interbank Financial Telecommunication) uses a designated communication method (Public Notice of the Financial Services Agency No. 11 of 2008) prescribed in Article 4, paragraph 1, item 9 of the Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds.

	through Methods Other Than Cash		
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.[*1])	(v)
13	Transactions with the National Government, etc. as a Customer	Transactions conducted by the national or a local government with the authority under laws and regulations as set forth in Article 4, paragraph 1, item 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.[*2]	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 Businesses that take telephone calls (including telecommunications by facsimile devices) to receive applications for contracts or to provide explanations about or consultation on goods, rights, or services or to provide the goods, rights or services, or for concluding such contracts. Specific examples of call center business include counters for material requests and inquiries, customer centers, help desks, support centers, consumer inquiry counters, maintenance centers, and order reception centers.

*2 Regarding agent work, etc. for specified mandated acts pertaining to the management or disposition of property listed in item 3 of the middle column of the row of persons listed in Article 2, paragraph 2, item 46 in the attachment to the Act on Prevention of Transfer of Criminal Proceeds, cases where the value of the said property is 2 million yen or less 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 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 non-profit 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 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.

Steady progress is underway towards achieving the targets of the above action plan. However, to adapt to changes in situations in and outside Japan, in the future AML/CFT/CPF measures will need rapid and continuous strengthening through collaboration between the relevant ministries and agencies under the supervision of the Inter-Ministerial Council.

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 therewith, and further reviewing those risks.

For its part, the Government of Japan will need to implement AML/CFT/CPF measures in collaborations 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.