Tentative Translation

December 2021

National Risk Assessment-Follow-up Report

National Public Safety Commission

Legal Abbreviations

Abbreviations for laws are as follows.

[Abbreviation]	[Law]
Foreign Exchange Act	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[*1] and terrorist financing (hereinafter referred to as "ML/TF") are constantly changing. In order to strongly cope with the problem, global countermeasures are required through cooperation of countries.

In the FATF[*2] Recommendations[*3] revised in February 2012, the Financial Action Task Force (FATF) requests countries to identify and assess ML/TF risks in their countries.

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[*4], 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[*5],etc. in keeping with the contents of the NRA-Baseline Analysis. [*6]

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 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

---

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

*2 Abbreviation of the Financial Action Task Force. It is an intergovernmental body established to promote international cooperation regarding Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) systems or controls.

*3 FATF sets out measures that countries should take, in the areas of law enforcement, criminal justice, and financial regulation to fight against ML/TF, as the FATF Recommendations.

*4 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.

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

*6 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.

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 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 set by the competent authorities. When the transaction is conducted with a particular specified business operator, it is also useful to look into factors affecting the risks and the status of the AML/CFT systems, relating to the products and services handled by the transaction counterpart, 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, specialized fraud 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 of specified business operators, which are dealt with by deposit taking institutions, funds transfer service providers, and crypto-assets exchange service providers, are assessed as relatively higher risk transactions than other business forms.

---

*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. Specialized fraud groups 3. Crime groups of foreigners in Japan	1. Predicate offences (thefts, frauds, etc.) 2. Major transactions misused for money laundering, etc.	1. Number of 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 is a national or local government, etc. 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

In the 2020 NRA-FUR, a new section has been added to describe the environment in Japan and review various risks related to ML/TF surrounding Japan. In addition, the criminal circumstances related to the COVID-19 was described due to the spread of the virus around the world. As for examples of cleared cases using STRs in the investigation of initiated cases, those using STRs from more diversified specified business operators were described for the purpose of promoting further understanding of AML/CFT measures and more efforts by specified business operators. Descriptions on quasi-Boryokudan and international terrorists were also deepened.

This NRA-FUR has enriched descriptions on legal persons that are not clearly identified, funds transfer services, crypto-assets that were misused for money laundering, and information on STRs related to such cases, etc. to indicate specific perspectives related to AML/CFT measures. In light of the recent criminal circumstances, the NRA-FUR has enriched descriptions on cybercrimes. It also introduced transactions of illegal wild life trade, which has drawn attention internationally, as well as international circumstances surrounding crypto-assets by referring to overseas reports.

In addition, as in the 2020 NRA-FUR, this NRA-FUR has updated the descriptions on information related to STRs used in the cleared cases to show how information on suspicious transactions reported by specified business operators is utilized in the investigation of money laundering, predicate offenses, etc., and also updated the descriptions on main matters to which specified business operators should pay attention and efforts on AML/CFT measures made by competent authorities and specified business operators in light of the actual circumstance confirmed by the competent authorities.

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), specialized fraud groups, and crime groups of foreigners in Japan, and predicate offenses such as theft and fraud that generate criminal proceeds.

---

*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.

○ Vulnerability

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

○ Consequence

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.

(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 by taking into account the findings pointed out in the Fourth Round of Mutual Evaluation of Japan.

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.

[Findings Pointed out in FATF Fourth Round of Mutual Evaluation of Japan]

In the report of the FATF Fourth Round of Mutual Evaluation of Japan published in August 2021, the following factors were pointed out regarding the technical compliance, effectivity, etc. of the AML/CTF measures in Japan:

○ Japan has a good understanding of the main elements of money laundering (ML) and terrorism financing (TF) risks, mainly based on the large number of assessments conducted. There are, however, a number of areas where the national risk assessment (NRA) and other assessments could be further improved. The assessment and understanding of TF risk is well demonstrated by counter-terrorism experts, but this does not extend to other Japanese officials with a role in CFT. National policies and strategies have sought to address some of Japan's higher risks, including virtual asset risks. However, these lack targeted AML/CFT activities. There is generally good interagency co-operation amongst most law enforcement agencies (LEAs) on AML/CFT operational matters, but more coordination is needed for the development of AML/CFT policies.

---

*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.

- Some financial institutions (FIs) have a reasonable understanding of their ML/TF risks, including bigger banks (such as global systematically important banks, which are identified as higher risk institutions) and some MVTS. Other FIs have a limited understanding of their ML/TF risks. Where FIs have a limited understanding of ML/TF risks, this has a direct impact on the application of the risk-based approach (RBA). They do not have an adequate understanding of the recently introduced/modified AML/CFT obligations, and have no clear deadlines to comply with these new obligations. Designated non-financial businesses and professions (DNFBPs) have a low level of understanding of ML/TF risks and of their AML/CFT obligations. Virtual asset service providers (referred to as virtual currency exchange providers (VCEPs)) have general knowledge about the crime risks associated with virtual assets (VA) activities and apply basic AML/CFT requirements. Suspicious transaction reporting (STR) is increasing, with a majority of reports from the financial sector and good reporting records from VCEPs, but overall STRs tend to refer to basic typologies and indicators. Not all DNFBPs are under an obligation to report, including some facing specific ML/TF risks.

- Understanding of risk by the different financial supervisors is uneven but is adequate for the most part. The Japanese Financial Services Agency (JFSA), the main financial sector regulator and supervisor, has taken relevant initiatives from 2018 that led to an improvement of its understanding of risks. The application of a risk-based approach (RBA) is still at an early stage, including for JFSA and the depth of its AML/CFT supervision is gradually improving. JFSA showed that once it engages in a dialogue with an FI, there is a tight follow-up process. Financial supervisors, including the JFSA, have not made use of their range of sanctions to take efficient and dissuasive actions against FIs. Japan has implemented a targeted and timely regulatory and supervisory response to the VCEP sector. The conduct of supervision based on ML/TF risks needs to be improved, noting that the JFSA has taken swift and robust actions to address VCEP deficiencies. DNFBP supervisors have a limited understanding of ML/TF risks and do not conduct AML/CFT supervision on a risk-basis.

- Japan has taken important steps towards implementing a system that allows competent authorities to obtain beneficial ownership (BO) information, with all FIs and DNFBPs obliged to maintain BO information. Nevertheless, accurate and up-to-date BO information is not yet consistently available on legal persons. There are challenges in relation to the transparency of domestic and foreign trusts, in particular trusts that are not created by or administered by trust companies. LEAs do not appear to have the necessary tools to establish the BO associated with more complex legal structures, and the risks associated with legal persons and arrangements are not well understood.

- Financial intelligence and related information are widely developed, accessed and regularly used to investigate ML, associated predicate offenses and potential TF cases. This is based on Japanese LEAs' own intelligence development and a good range and quality of intelligence developed by the FIU (JAFIC). JAFIC adds value in complex financial investigations. LEAs tend to use financial intelligence to support targeting suspects and understanding the connections between them, but use for tracing assets requires further enhancement.

- ML investigations pursued by Japanese LEAs are in line with some of the key risk areas. LEAs demonstrated extensive experience with investigating less complex ML cases and some experience of conducting complex investigations in particular organized crime targets and ML cases involving foreign predicate offenses. There are particular challenges in investigating larger scale ML cases of cross-border and domestic drug trafficking. All ML prosecutions that have been undertaken have secured a conviction. However, authorities are only prosecuting ML in line with the overall risk profile to some extent. Custodial sentence available for ML are at a lower level than those available for the predicate offenses most regularly generating proceeds of crime in Japan. In practice, sanctions applied against natural persons convicted of ML are generally in the lower end of the range. Suspended sentences and a fine are often imposed.

- Restraint and confiscation are well demonstrated in relation to fraud cases, but not for some other high risk ML predicates. Japan pursues a generally successful approach to confiscating instruments of crime, with the exception of the large amounts of seized gold. Challenges arise with the confiscation of proceeds, instrumentalities and property of corresponding value from the overall level of suspended prosecutions (predicates and ML). Despite the cross-border cash smuggling risks, Japan has yet to demonstrate effective detection and confiscation of falsely/not declared cross-border movements of currency.

- Japan provides constructive and timely international cooperation. Domestic processes for responding to mutual legal assistance (MLA) requests operate well. Japan has provided assistance to other countries in confiscating property of equivalent value in Japan, although it has limited experience with assets being repatriated from other jurisdictions. Japan has demonstrated its ability to execute extradition requests from other jurisdictions, although the judicial framework for extradition should be reinforced. Japan routinely uses other forms of international

cooperation in a timely manner, for exchanges of information relevant to AML/CFT functions including supervision, ML and predicate investigations.

- Japanese LEAs effectively investigate and disrupt potential TF, using information and financial intelligence from a wide range of sources. However, deficiencies in the TF Act, and a conservative approach to prosecution (see IO.7 above) constrain Japan's ability to prosecute potential TF and punish such conduct dissuasively. Japan has a limited understanding of at-risk non-profit organizations (NPOs), which has impeded competent authorities' ability to conduct targeted outreach to bolster NPOs' CFT preventive measures. This has placed Japanese NPOs at risk of being unwittingly involved in TF activity.
- Japan implements targeted financial sanctions (TFS) with delays, which have been significantly reduced as a result of recent administrative changes to the process used to implement designations. A number of other measures targeting the proliferation of Weapons of Massive Destruction (WMD) by DPRK, including comprehensive restrictions on trade and domestic designations, mitigate delays to some extent. This is particularly important due to Japan's context. Nevertheless, while screening obligations require FIs, DNFBPs and VCEPs to implement TFS without delay, there are weaknesses in the implementation of TFS by FIs, VCEPs and DNFBPs. Authorities demonstrated good inter-agency cooperation and coordination on intelligence and law enforcement activities related to combating WMD, and effective and proactive outreach to some specific private sector entities at particular risk of unwittingly facilitating sanctions evasion.

Measures to lower the risks have been examined or taken according to the action plan published in the same month to strengthen the AML/CTF measures in Japan based on the findings pointed out above.

Section 2. Environment surrounding Japan

This NRA-FUR analyzes money laundering cases (offenders and modus operandi) and other cases, as well as risks associated with products and services, cross-sectionally in and after *Section 3. Analysis of Money Laundering Cases, etc.* based on the analysis of various risks related to ML/TF surrounding Japan described in this Section. As a result of the analysis, high-risk transactions are identified from the viewpoints of transaction types, countries/regions, customer attribute, and products and services. A multifaceted and comprehensive risk assessment is conducted based on the situation for the measures taken to mitigate the identified risks.

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[*1] nationwide, immigration control and customs procedures are conducted from the viewpoints of preventing terrorism and smuggling committed by international criminal groups.

2. Social Environment

According to the preliminary results of the population census (Statistics Bureau, Ministry of Internal Affairs and Communications), Japan's total population as of October 1, 2020, was 126,227,000, a decrease of 1.4% compared with the statistics ten years ago (2010). On the other hand, according to the population estimate (Statistics Bureau, Ministry of Internal Affairs and Communications), the aging rate as of October 1, 2020 (the ratio of the population aged 65 and over to the total population) reached a record high of 28.8%[*2], an increase of 5.8 points compared to the aging rate of 23.0%[*3] ten years ago. It is at the highest level compared to other developed countries. In the future, it is estimated that the aging of the population will progress further as the population aged 65 and over will increase while the total population will decrease.

In Japan, where the birthrate is declining and the population is aging rapidly, some industrial fields have difficulty securing human resources to address the severe labor shortage issue, even though efforts have been made to improve productivity and secure domestic human resources. In such fields, it is necessary to build a mechanism to accept work-ready foreign nationals who have a certain degree of expertise and skills. Therefore, two statuses of residence of Specified Skilled Worker (i) and Specified Skilled Worker (ii) were established by the Act for Partial Amendment of the Immigration Control and Refugee Recognition Act and the Act for Establishment of the Ministry of Justice (Act No. 102 of 2018). For the number of foreigners entering Japan, refer to the *Status of Entry/Residence of Foreigners in Japan* on page 16.

3. Economic Environment

Japan's economy is facing difficulty due to the influence of the novel coronavirus infection. However, even under such circumstances, Japan occupies a vital position in the world economy. The nominal GDP in 2020 (Quarterly Estimates of GDP for Apr.-Jun. 2021 (The Second Preliminary Estimates)) was 538.7 trillion yen, the third-largest economy after the United States and China. In terms of purchasing power parity GDP in 2019, it is the fourth largest globally after China, the United States, and India. The real GDP growth rate in FY2020 was -4.4%. The share of the composition ratio of nominal GDP by economic activity in 2019 was 1.0% for the primary industry, 26.0% for the secondary industry, and 73.0% for the tertiary industry. Regarding the trade value in 2020, Japan's exports amounted to 68,400.5 billion yen, and imports amounted to 67,837.1 billion yen. The main export partners were China, the United States, and South Korea, etc., and the import partners were China, the United States, and Australia, etc.

---

*1 The number of seaports and airports listed in Appendix 1 of the Ordinance for Enforcement of the Immigration Control and Refugee Recognition Act is 127 and 32, respectively. The number of seaports and airports listed in Appendix 1 and 2 of the Ordinance for Enforcement of the Customs Act is 119 and 32, respectively.

*2 Estimated value based on the 2015 population census

*3 Based on the 2010 population census (population divided proportionally by people of uncertain age).

In Japan, foreign transactions are conducted freely. However, economic sanctions by international cooperation and economic sanctions by Japan alone are being implemented with consideration of North Korea's missile launches, nuclear tests, and Iran's nuclear development, 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 September of 2020, the number of branch offices of major financial institutions[*1] was 37,587 (including 174 overseas branch offices). There were 95,266 ATMs 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 2020 were Japanese megabanks.

In terms of the scale of financial transactions in Japan, the balance of bank deposits at the end of March of 2021 was approximately 896 trillion yen. As for settlement transactions, the handling status of domestic exchange (other banks' transaction volume of exchange) in 2020 was approximately 2,927 trillion yen (approximately 1.7 billion cases), and the daily average was about 12 trillion yen (approximately 7.13 million cases). The amount of foreign exchange in yen settlement during the same year was approximately 4,427 trillion yen (approximately 6.72 million cases), and the daily average was approximately 18 trillion yen (approximately 30,000 cases).

Next, regarding the securities market size, Japanese stocks' market capitalization was approximately 694 trillion yen as of December of 2020. In terms of market capitalization classified by country, Japan ranks third after the United States and China. The Tokyo Stock Exchange is the third-largest exchange globally after the New York Stock Exchange and the NASDAQ Stock Exchange. Furthermore, the trading value of listed stocks held on the Tokyo Stock Exchange in 2020 was approximately 682 trillion yen.

As for cash transactions, as mentioned above, there are many branches and ATMs of financial institutions. Therefore, it is convenient to withdraw cash from deposit accounts or to deposit money into accounts. Furthermore, there is "adequate security" with few thefts and people who lost money get them returns very often. There is also "a high level of trust in cash" with 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 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 (see *Section 5. Risk of Products and Services*), 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

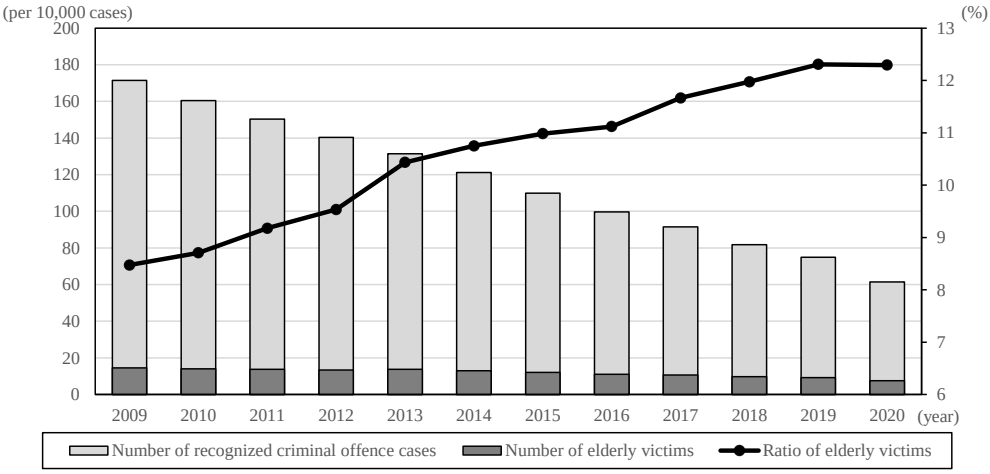
Among the indicators for measuring Japan's criminal circumstances, the total number of recognized criminal offense cases was 614,231 in 2020, which continues to be a record low after the war as in the previous year. The number decreased by 17.9% from the previous year, and the rate of decrease is more than most years (in 2019, the number decreased by 8.4% from 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 78.5% (the total number of cleared criminal offenses was 279,185, and although it continued to decline, the rate of arrests was 45.5%, up 6.2 points from the previous year). On the other hand, offenses associated with the spread of virus such as thefts at stores, etc. which have suspended business by responding to the business suspension request, etc. made as part of the emergency measures taken by the government and frauds related to the COVID-19 have been found. Offenses misusing economic support for business operators such as fraud for stealing relief payment related to the spread of virus have also occurred.

The number of elderly victims to the number of recognized criminal offenses has consistently increased since 2009. In 2020, it was 12.3%, up 3.8 points from 8.5% in 2009 (see Table 1).

---

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

Table 1 [Number of Recognized Criminal Offense Cases and Ratio of Elderly People among Victims, etc.]



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 31.0% in 2020, an increase of 15.6 points from 2010. Furthermore, in terms of the damage to the elderly by specialized fraud groups, which are the main offenders of money laundering in Japan (see *Section 3. Analysis of Money Laundering Cases of this NRA-FUR*), the ratio of damage to the elderly (excluding damage to companies) to the total number of recognized cases of specialized fraud was 85.7% in 2020 (see Table 2).

Table 2 [Number of Recognized Cases of Elderly Victims for Each Type of Specialized Fraud (2020)]

	It's me fraud	Deposit fraud	Billing fraud	Refund fraud	ATM Card fraud	Other fraud	Total
Number of recognized cases	2,136	4,069	915	1,581	2,757	129	11,587
Ratio of elderly victims for each type (excluding damage to companies)	94.0%	98.4%	45.6%	87.7%	96.7%	28.9%	85.7%

Next, looking at the number of cleared cases of cybercrime, which has been increasing in recent years, the number was the highest ever in 2020 (9,875 cases) (see Table 3). Although the amount of loss from online banking fraud decreased significantly from the previous year, there was only a slight decrease in the number of cases, which still remains high. Similar to the previous year, short message services (SMS) and emails are believed to have been used in many cases to lead the victims to phishing sites disguised as financial institutions (see Table 4).

Table 3 [Status of Cybercrime Arrests]

	2016	2017	2018	2019	2020
Number of cleared cases	8,324	9,014	9,040	9,519	9,875

Table 4 [Number of Online Banking Fraud]

	2016	2017	2018	2019	2020
Number of cases	1,291	425	322	1,872	1,734

In 2020, there were many cases in which systems, etc. were infected with ransomware (illegal program for demanding ransom) through attacks on the vulnerabilities in software or systems and through targeted emails. The significant loss caused by ransomware and the maliciousness of this crime are becoming a problem in the world. In Japan, the system of a leading company was infected with ransomware in November 2020. The personal information retained by the company was stolen and encrypted. The company was asked to pay ransom in exchange for not disclosing the information. This method is called double extortion. According to

the research[*1] results announced by a security company in 2020, the amount of loss from ransomware (including loss from the suspension of business and operational costs and excluding the payment of ransom) suffered by Japanese companies is the second highest in the world, which shows the severity of ransomware attacks in Japan. The number of accesses considered to be search activities in cyberspace detected by the National Police Agency is also rising. The threat in cyberspace in Japan has become a serious issue.

(2) Terrorism Situation

As for international terrorist situation, ISIL[*2] calls on sympathizers to carry out terrorism against Western and other countries participating in the Global Coalition to Counter ISIL. Besides, AQ[*3] 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, it is necessary to pay attention to changes in terrorism threats in and outside Afghanistan. Terrorist attacks have occurred one after another in various parts of the world. There have also been cases in which Japanese people and interests of Japan related facilities have been damaged overseas by terrorism. Therefore the threat of terrorism against Japan still exists. Although many years have passed since the alleged abduction by North Korea, not all victims have yet return to Japan, and no respite is allowed.

In addition to this situation, cyberattacks targeting government agencies and companies are occurring globally in cyberspace. There is also concern that cyber terrorism, an electronic attack that paralyzes society's functions, will occur in Japan.

---

*1 Sophos State of Ransomware Report 2020

*2 Acronym of the 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.

*3 Abbreviation for Al-Qaeda

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), specialized fraud 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 2020, 58 cases (9.7%) were related to Boryokudan members, associates and other related parties (hereinafter referred to as "Boryokudan gangsters") (see Table 5). Out of those, 57 cases fell under the Act on Punishment of Organized Crimes, Control of Crime Proceeds and Other Matters (27 for concealment of criminal proceeds and 30 for receipt of criminal proceeds) and one fell under the Anti-Drug Special Provisions Law (one for concealment of illegal drug proceeds).

When looking at the number of cleared cases of money laundering between 2018 and 2020 in which Boryokudan gangsters were involved in relation to predicate offenses, the majority was fraud and loan shark.[*2] On the other hand, when looking at the number of Boryokudan gangsters as a proportion of arrested offenders in relation to predicate offenses, it appears that their ratio in gambling, blackmailing, illicit drugs, and prostitution offenses is high.

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.

With respect to Boryokudan, this NRA-FUR also explains the results of surveys and analyses in "Anti-social Forces (including Boryokudan)" under *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes*.

Table 5 [Number of Cleared Money laundering Cases (Committed by Boryokudan Gangsters) under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law]

Year / Category	2018	2019	2020
Cleared cases of money laundering offenses	511	537	600
Cases by Boryokudan gangsters	65	58	58
Percent (%)	12.7%	10.8%	9.7%

*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) Specialized Fraud Group

In recent years, the number of recognized specialized fraud cases[*1] and the amount of loss suffered have remained high (see Table 6). Damage in 2020 was concentrated in metropolitan areas. Tokyo (2,896 cases) accounted for 21.4% of the total number of cases recognized, and seven prefectures, including Kanagawa (1,773 cases), Chiba (1,217 cases), Osaka (1,107 cases), Hyogo (1,027 cases), Saitama (1,026 cases), and Aichi (569 cases), accounted for 71.0% of the total number of cases recognized. Having the ringleader as the core, specialized fraud 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, vehicles, etc., and the existence of foreign crime bases has surfaced.

Furthermore, there are some people who make bank accounts in the name of fictitious or third parties by using falsified identifications and thoughtlessly sell their own bank account to obtain funds for amusement expenses or the cost of living. Such people make money laundering easier.

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 specialized fraud. Based on this, the police are promoting various measures to eradicate specialized fraud 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 6 [Number of Recognized Specialized Fraud Cases and Total Financial Damage]

Category \ Year	2018	2019	2020
Number of recognized cases	17,844	16,851	13,550
Total financial damage (yen) (Effective total amount of financial damage)	38,286,761,222	31,582,937,585	28,523,359,039

Note 1: Data from the National Police Agency
2: Since 2018, there have been reported cases where criminals deceive their victims by phone and get them to bring their cash cards, then secretly swaps them with another card when the victims are not looking. Although the name of this offense is theft, it can essentially be treated like a type of "It's me fraud" that delivers cash cards by hand. To more accurately grasp the extent of this type specialized fraud, theft using this modus operandi has been counted as specialized fraud since the 2018 statistics.
3: 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).

Table 7 [Location of Bases of Criminals Arrested in 2020]

Tokyo	Osaka	Chiba	Saitama	Kyoto	Ehime	Fukuoka	Total
19	5	2	1	1	1	1	30

*1 Specialized fraud is the collective term for offenses that involve defrauding the victim of cash or other valuables (including extortion of cash, or stealing of cash cards or other valuables when the opportunity arises) by phone calls to an unspecified large number of persons and gaining their trust without meeting them in person, thereby persuading them to transfer money into a specified savings account, or through other methods.

(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 2020, 79 cases (13.2%) were committed by foreigners in Japan (see Table 8). The breakdown comprised 1 case of controlling business administration of corporations, etc., 58 cases of concealment of criminal proceeds, and 20 cases of receipt of criminal proceeds.

Table 8 [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	2018	2019	2020
Cleared cases of money laundering offenses	511	537	600
Cases by foreigners	48	71	79
Percent (%)	9.4%	13.2%	13.2%

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; there were money laundering cases associated with cases of illegal remittance pertaining to Internet banking systems committed by a group of Chinese , shop lifting by a group of Vietnamese, and international fraud by a group of Nigerians.

As for the number of people arrested for illegal transfers, etc., of deposit books, cash cards, etc., in violation of the Act on Prevention of Transfer of Criminal Proceeds in the last three years, Vietnamese and Chinese nationals accounted for more than 80% of the total.

In addition, with respect to the number of STRs in the last three years, STRs related to Vietnamese, Chinese, and Koreans ranked the highest among other nationalities. Recently there has been a remarkable increase in reports related to Vietnamese.

With respect to international transactions, this NRA-FUR also contains the results of surveys and analyses in "International Transactions" under *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes*.

The box below shows the status of the entry/residence of foreigners and the situation concerning crimes committed by foreigners in Japan.

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

[Status of Entry/Residence of Foreigners in Japan]

The number of foreigners entering Japan in 2020 was 4,307,257. Of these, the total number of new arrivals was 3,581,443, approximately 25,000,000 (87.4%) less compared to the previous year because of the government's measures against the spread of COVID-19 (it is about the same as the number of new arrivals in 1996). As far as the number of new arrivals by nationality and region is concerned, the number of Chinese was the largest, accounting for more than 20%, followed by Taiwanese, Koreans, Chinese (Hong Kong), and Thais; the number of Asians accounts for 80% of the total number of new arrivals. As for the purpose of entry (status of residence), the number of Temporary Visitors was the largest (3,360,831), accounting for 93.8% of the total number of new arrivals, followed by foreigners with the status of residence of Technical Intern Training (i) (76,456), status of residence of Student (49,748), and status of residence of Engineer/Specialist in Humanities/International Services (19,705), accounting for 2.1%, 1.4%, and 0.6%, respectively. As for the new arrivals with the status of residence of Technical Intern Training (i) (which has been high in recent years) by nationality and region, the number of Vietnamese was the largest (41,341), accounting for 54.1%, followed by Chinese (14.5%), Indonesians (10.8%), Filipinos (6.7%), and Thais (3.6%).

Next, in terms of the number of foreign residents as of the end of 2020, the number of mid-to-long term residents in Japan (excluding permanent residents, and hereinafter the same) was 1,775,169. It was an increase of more than 50% from 10 years before. The ratio of mid-to-long term residents to Japan's total population at the end of 2020 was 1.41% of the total population of 126.23 million [as of October 1, 2020, population census (Statistics Bureau, Ministry of Internal Affairs and Communications)], which is 0.53 points higher than ten years before. In terms of the number of mid-to-long term residents by nationality and region as of the end of 2020, Chinese accounted for 27.8% of the total (494,035 residents), followed by Vietnamese 24.2%, Filipinos 8.2%, Brazilians 5.4%, and Nepalese 5.1%.

[Recent situation concerning crimes committed by foreigners in Japan]

Although the total number of cleared cases involving foreigners in Japan (the numbers of cleared cases of Penal Code offenses and special law offenses) as well as the number of offenders arrested (the numbers of offenders arrested for Penal Code offenses and special law offenses) have remained relatively stable in recent years, they are on a slightly upward trend because the number of cleared cases and the number of offenders arrested for special law offenses have increased. In 2020, Vietnamese and Chinese accounted for about 60% of the total number of cleared cases and total number of offenders arrested, and Vietnamese has the highest ratio to the total. In terms of the total number of offenders arrested in 2020 (11,756) by nationality and region, Vietnamese accounted for 35.9% (4,219), followed by Chinese 23.0% (2,699), Filipinos 6.5% (765), Brazilians 4.3% (508), and Thais 4.1% (480). As for the total number of offenders arrested by type of crimes and violations of laws and regulations, violations of the Immigration Control Act and thefts account for the highest percentage (see Table below).

Table [Number of Offenders Arrested by nationality, for Penal Code offenses and Special law violations (2020) (top 5 countries)]

Nationality and Region	Vietnam	China	Philippines	Brazil	Thailand
Total offenders arrested	4,219	2,699	765	508	480
Penal Code offenses	1,495	1,473	335	351	60
Larceny	873	687	127	122	26
Violence	145	302	118	141	20
Intellectual offenses	76	193	17	12	4
Felonious offenses	55	25	8	26	2
Moral offenses	19	35	14	7	0
Other offenses	327	231	51	43	8
Special law offenses	2,724	1,226	430	157	420
Immigration Control Act	2,332	846	292	12	368
Drug-related offenses	141	19	66	101	17
Fire Arm Control Act	44	36	6	12	1
Moral Control Act	1	73	15	0	23
Anti-prostitution Act	0	5	0	0	0
Other law	206	247	51	32	11

In terms of the total number of arrested offenders by status of residence, Technical Intern Training account for 24.6% (2,889), followed by Student 17.7% (2,085), Short-term Stay 15.5% (1,824), etc. The total amount of loss from offenses against property by foreigners in Japan arrested in 2020 was 1.9 billion yen, of which about 1.4 billion yen (71.8%) was from thefts, and about 0.5 billion (26.7%) was from frauds, etc. Looking at the cleared cases for "crime infrastructure"-related offenses, we see that the criminals forged passports, residence cards, etc., so as to provide foreigners a status of residence that would allow them to work; thus the number of arrests has been on the rise and reached its height in 2020.

In recent years, most Vietnamese crimes have been theft, with shoplifting being the most common method. Murders have occurred from quarrels among Vietnamese, as well as kidnapping and abduction occurring in connections to 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 stay for work or pretend to be legal residents by obtaining a fake residence card after their authorized period of stay has expired.

Chinese offenders use a highly anonymous smartphone app as their communication method. There are relatively many cleared cases in which they use well-made fake credit card, etc., to steal a large quantity of products or to commit "crime infrastructure"-related offenses, such as forgery of passports and residence cards.

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. The following are examples of money laundering cases involving Chinese nationals:

- A case where an offender concealed the criminal proceeds obtained through unauthorized access to Internet bank accounts by transferring them to multiple illegally obtained accounts under the name of Vietnamese persons
- A case where an offender concealed the criminal proceeds obtained through illegal reselling of pharmaceutical products by transferring them to an account under the name of an acquaintance of the offender
- A case where an offender concealed the proceeds from the sales of forged brand-name goods by transferring them to illegally obtained accounts under the name of a Japanese person
- A case where an offender sold fraudulent products that were different from the expensive products that he/she presented to customers on social media, and concealed the criminal proceeds by having the customers wire the amount corresponding to the value of the expensive products to an account under the name of another party

2. The following are examples of money laundering cases involving Vietnamese nationals:

- A case of operating an underground bank by using an SNS to accept requests to remit money overseas and then have the money transferred to accounts opened in Japan under the name of another party
- A case where the proceeds from the sales of forged residence cards were transferred to accounts under the name of other parties
- A case where a Vietnamese illegally staying in Japan took advantage of a mobile phone company's compensation policy by pretending to be a subscriber, whose mobile phone was broken, in order to claim a new one. The offender later sold the phone and concealed the proceeds from the sale by having the money wired to an account under the name of another party

3. The following are examples of money laundering cases involving other foreigners in Japan:

- A case where Nigerians and others sent bogus emails to an American company and tricked them into transferring money to an account opened in Japan under the name of a legal person, thereby concealing criminal proceeds
- A case where Nigerians and others deceived women whom they met through social media into remitting money to an account opened in Japan under the name of another party, thereby concealing criminal proceeds
- A case where a Malaysian acted upon instructions from his handler via SNS to receive forged credit cards stored in coin-operated lockers

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. In June 2017, the Act on Punishment of Organized Crimes was revised to substantially increase the types of predicate offenses. They include offenses that generate illegal proceeds and those subject to the death penalty, imprisonment with work for life or 4 years or longer, or imprisonment without work, 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. Among them are murder, robbery, theft, fraud, breach of trust and other criminal offenses, as well as offenses subject to the Immigration Control and Refugee Recognition Act, the Investment Act, the Anti-Prostitution Act (Act No. 118 of 1956), the Trademark Act (Act No. 127 of 1959), the Banking Act (Act No. 59 of 1981), the Copyright Act (Act No. 48 of 1970) and the Firearms and Swords Control Act.

Among cleared money laundering cases categorized as predicate offenses in 2018–2020[*1], theft was the leading crime with 624 cases, accounting for 37.0%, followed by fraud (523 cases for 31.0%), computer fraud (129 cases for 7.6%), violation of the Investment Act/Money Lending Business Act (86 cases for 5.1%), and violation of the Immigration Control and Refugee Recognition Act (36 cases for 2.1%) (see Table 9).

Table 9 [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 place for profit	Violation of the Anti-Prostitution Act	Violation of the Trademark Act	Illicit drugs	Distribution of obscene material, etc.	Extortion	Embezzlement	Violation of the Amusement Business Act	Armed robbery	Document forgery offenses	Violation of the Banking Act	Others	Total
Number of cases	624	523	129	86	36	32	29	25	20	20	20	20	17	15	14	13	65	1,688
Ratio (%)	37.0	31.0	7.6	5.1	2.1	1.9	1.7	1.5	1.2	1.2	1.2	1.2	1.0	0.9	0.8	0.8	3.8	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 international crime organizations were involved in some of the predicate offenses, resulting in cross-border money laundering. With respect to international transactions, this NRA-FUR also explains the results of surveys and analyses in "International Transactions" in *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes*.

Major predicate offenses are analyzed below.

---

*1 There were 1,648 cleared cases of money laundering under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law from 2018 to 2020. On the other hand, the total number of cleared money laundering cases counted by predicate offenses was 1,688 (See Table 9) because some money laundering cases can be counted in multiple predicate offenses.

A. Theft

(a) Forms of offenses

As for theft, there are cases where the amount of financial damage is comparatively small, but there are also cases committed continuously and repeatedly by crime organizations, including Boryokudan and crime groups of foreigners in Japan, that result in large amounts of criminal proceeds.

For example, there were cases where members of multiple Boryokudan organizations were involved, and a large amount of cash was withdrawn from ATMs in multiple convenience stores, etc. illegally using forged cards containing customer information issued by oversea banks. In addition, there were cases of shoplifting offenses, which accounts for the majority of the offenses committed by Vietnamese, which have been on the rise recently. Typically, they involve groups whose members take specific roles of giving instructions, executing the crime, transporting, etc. For example, one offender gives instructions via SNS from Vietnam to shoplift a large quantity cosmetics and pharmaceutical products, others carry out the theft itself, another offender poses as an export agent to send the stolen products to Vietnam, or another acts as a tourist to carry the stolen goods out of Japan by hand. Regarding organized car theft committed by Boryokudan and crime groups of foreigners in Japan, there were cases where stolen cars were carried to so-called yards surrounded by iron walls, disassembled and then illegally exported overseas.

The total financial damages from theft during 2020 was about 50.2 billion yen (about 16.8 billion yen for the total amount of damage in cash), generating a large amount of criminal proceeds.

(b) Modus operandi of money laundering

Regarding the modus operandi of money laundering offenses related to theft as predicate offenses, the following cases, etc. have occurred:

- Cases of buying and keeping stolen cars knowing that they were stolen;
- Cases where a large number of coins obtained via burglary were deposited into an account under the name of another party and an amount equivalent to the coins were withdrawn afterwards, resulting in factual exchange;
- Cases where a large quantity of stolen gold ingots was sold to a gold trader in the name of a legal person operated by a friend of the offender;
- 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; and
- Cases where cash was withdrawn and stolen by using an illegally obtained cash card, and hiding the cash in a coin-operated locker.

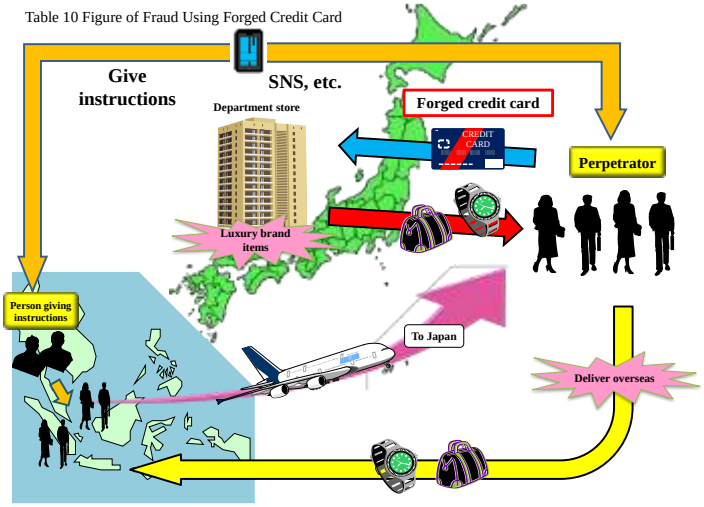
B. Fraud

(a) Forms of offenses

Fraud offenses, including specialized fraud 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.

For example, there are cases where Boryokudan commit specialized fraud, where the proceeds of a fraud offense committed outside Japan by an international criminal group were brought into Japan from overseas through an account opened at a Japanese financial institution, where a foreigner in Japan brought in a forged credit card from outside Japan and used the card to fraudulently buy luxury brand items from department stores in Japan (see Table 10), and where products are obtained fraudulently by pretending to be an authorized user of a code payment service by using an illegally obtained ID and password.

Table 10 Figure of Fraud Using Forged Credit Card



The total financial damages from fraud offenses in 2020 was about 64.0 billion yen (Total damages in cash were about 59.2 billion yen). Although the total damages from theft offenses exceed those from fraud offenses, the average financial damage due to each case of fraud is about 2.10 million yen bigger than that of a theft offense (about 120,000 yen). In particular, specialized fraud offenses generate a large amount of criminal proceeds with an average about 2.20 million yen per case.

(b) Modus operandi of money laundering

Regarding the modus operandi of money laundering offenses related to fraud as predicate offenses, the following cases, etc. have occurred:

- Accounts under the name of individuals sold to crime groups when foreigners leave Japan were misused as accounts for receiving money stolen through specialized fraud;
- Accounts under the name of fake companies established for receiving proceeds from specialized fraud were opened and misused; and
- Accounts under the name of individuals with business names opened for receiving proceeds from fraud in foreign countries were misused.

In many cases, damages from specialized 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 immediately after the transfer, remitted to other accounts, or transferred through multiple accounts opened under another person's name. This is done to prevent financial institutions or the like from freezing the accounts once they have detected the damages. 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 specialized fraud offenses, etc.

C. Computer fraud

(a) Forms of offenses

Regarding computer fraud, there are cases where offenders operate ATMs by using the illegally obtained cash cards of others, or IDs and passwords for online banking to illegally access the business system managed by financial institutions and transfer money from accounts of victims to accounts managed by the offenders. Some of the cash cards used in computer fraud were illegally obtained through specialized fraud.

Regarding online banking fraud, most offenders are believed to illegally transfer money from bank accounts of victims by leading them to phishing sites disguised as financial institutions via short message services (SMS) or emails to steal their IDs, passwords, etc. There were also cases where offenders led victims to phishing sites disguised as financial institutions via SMS by pretending to be from courier companies or e-commerce companies that want to deliver packages, and cases where offenders got victims to install illegal apps in their mobile phones and lead them to phishing sites from fake messages indicated by the apps.

Of the 2,181 bank accounts identified as the primary destinations for illicit transfers in 2020, Japanese accounted for about 37.8% of the nationalities of the account holders, followed by Vietnamese (about 17.9%) and Chinese (about 2.4%).

As explained above, while Boryokudan involvement is observed in specialized fraud offenses, international criminal organizations have also been observed engaging in online banking fraud. The reality of the situation is that criminal organizations commit such offenses in an organized manner to obtain large amounts of criminal proceeds.

(b) Modus operandi of money laundering

Regarding the modus operandi of money laundering offenses related to computer fraud as predicate offenses, the following cases, etc. have occurred:

- The maximum amount of cash was withdrawn from ATMs using cash cards obtained via specialized fraud 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;
- A criminal organization in China illegally accessed the business system of a financial institution in Japan and transferred money to an account under the name of another person, and a Chinese criminal group in Japan withdrew cash from the account; and
- Crypto-assets obtained by fraudulent acts on the server of a crypto-asset wallet service were transferred to the anonymous account of a decentralized crypto-asset exchange managed by the criminal.

D. Violation of the Investment Act/Money Lending Business Act

(a) Forms of offenses

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 have not registered for the money lending business purchase the salary claims held by individuals (workers) against employers and provide them with money to collect the funds related to the claims through such individuals.

Large amounts of criminal proceeds are generated, and in 2020, the amount of damages reached over 4.3 billion yen, according to the statistics on cleared loan-shark crimes. In addition, it is recognized that Boryokudan repeatedly and continuously conduct loan sharking as an important source of revenue.

(b) Modus operandi of money laundering

Regarding the modus operandi of money laundering offenses related to loan-shark crimes as predicate offenses, the following cases have occurred:

- Debt repayments were remitted to accounts under the name of other parties to conceal debt repayments to the loan sharks. These accounts were obtained by the loan sharks as debt repayments from borrowers and illegally used to conceal criminal proceeds.

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. In other cases, loan sharks made borrowers issue bills and/or checks when borrowing, and if there was any delay in repayment, such bills and/or checks were brought to a financial institution and payment is made to an account under the name of another party. There was also a case where a fictitious sales agreement was made with the borrower and debt repayment was obtained by settling the deferred payment.

E. Violation of the Immigration Control Act

(a) Forms of offenses

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 human trafficking where an offender places foreigners under his/her control by taking away their passports, etc., and forcing them to work.

The number of cleared cases of violations of the Immigration Control Act was 6,534 in 2020, which is a 10.8% increase from the previous year, and the number of cleared cases of possessing forged residence cards, etc., was 790, which is the highest since 2013 when the statistic started being recorded.

(b) Modus operandi of money laundering

Regarding the modus operandi of money laundering offenses related to violations of the Immigration Control Act as predicate offenses, the following cases, etc. have occurred:

- The proceeds from the sales forged residence cards were transferred to accounts under the name of other parties; and
- Boryokudan members received cash as a protection fee knowing that the cash was criminal proceeds obtained through the promotion of illegal employment.

F. Habitual gambling/Running a gambling place for profit

(a) Forms of offenses

Regarding offenses related to habitual gambling and running a gambling place 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 where 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 place for profit. In 2020, the orders were issued for about 158.6 million yen in cash in connection with illegal gambling facilities.

(b) Modus operandi of money laundering

Regarding the modus operandi of money laundering offenses related to habitual gambling/running a gambling place for profit as predicate offenses, the following cases, etc. have occurred:

- 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
- Dividends were transferred to accounts under the name of another person in baseball gambling, etc.

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.

G. Violation of the Amusement Business Act/Violation of the Anti-Prostitution Act

(a) Forms of offenses

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 where offenders forced victims to engage in prostitution by using violence, intimidation, etc.

For the last three years, offenses related to violating the Amusement Business Act and the Anti-Prostitution Act rank high for the number of cases of temporary restraining order for confiscation before institution of prosecution as prescribed in the Act on Punishment of Organized Crimes.

(b) Modus operandi of money laundering

Regarding the modus operandi of money laundering offenses related to violations of the Amusement Business Act or the Anti-prostitution Act as predicate offenses, the following cases, etc. have occurred:

- Sales proceeds paid with credit cards were transferred to accounts under the name of other parties;
- Proceeds paid for arranging women for illegal adult-entertainment business, etc. were transferred to an account under the name of an offender; and
- A Boryokudan member received proceeds from prostitution through a bank account under the name of a family member

H. Narcotics-related crimes

(a) Forms of offenses

Regarding stimulant-related crimes, which account for more than 60% of all narcotics-related crimes, the quantity of stimulants confiscated in 2020 was 437.2 kg, a decrease from the previous year. However, the quantity of confiscation of smuggled stimulants was 418.2 kg, which is still a large amount. It can be assumed that smuggling and illicit trafficking of stimulants still generate a large amount of criminal proceeds.

Boryokudan gangsters, etc. accounted for at least 40% of the offenders in arrested cases of stimulant-related crimes during 2020. In terms of the number of persons arrested for stimulant-related crimes committed by Boryokudan gangsters, etc., classified by significant violation types, there were 2,109 use offenders, 1,142 possession offenders, 199 transfer offenders, 38 acquisition offenders, and 20 smuggling offenders. Furthermore, of the total number of stimulant profit-making offenders arrested (490), the number of Boryokudan gangsters, etc., arrested was 278, accounting for 56.7%. The situation Boryokudan is deeply involved in smuggling and illicit trafficking of stimulants has continued.

On the other hand, cannabis-related crimes, which account for more than 30% of all narcotics-related crimes, have been increasing since 2013. In particular, the number of young people arrested for cannabis-related crimes has increased significantly. Regarding cannabis-related crimes, of the total number of offenders cleared in profit-making offense cases (342), 83 were Boryokudan gangsters, accounting for 24.3% of the total. Boryokudan is still involved in the smuggling of cannabis. 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 2017, Boryokudan gangsters and Chinese offenders were arrested in a case where about 475 kg was seized. In 2019, Boryokudan gangsters and Taiwanese were arrested in a case where about 587 kg was seized.

As for overseas drug-related criminal organizations, the presence of Chinese, Mexican and West-African organizations is still large, and criminal proceeds from drug-related crimes are an important source of funds for overseas criminal organizations as well. The breakdown of cleared cases in 2020 of stimulant smuggling by origin shows that Malaysia and the U.S. occupy the largest share, followed by Thailand, Vietnam, Taiwan, U.K., and Mexico. The breakdown of foreigners in Japan arrested for offenses related to illicit stimulant trafficking by nationality shows that Korea, Brazil, Vietnam, and Iran occupy a large share. Looking at the number of offenders cleared for cannabis-related crimes in 2020 by country and region of origin, the U.S. occupied the largest share, followed by Canada, U.K., and France. Criminal proceeds related to stimulant trafficking and smuggling are likely to be transferred between countries that have different legal systems and transaction systems.

Regarding narcotic trafficking crimes in 2020, the number of cases where offenders engaged in narcotic trafficking by carrying them on airplanes has decreased, while the number of cases where they used international courier services or postal services has increased.

Table 11 [Number of Offenders Arrested for Stimulant and Cannabis-related Crimes]

Category \ Year		2018	2019	2020
Offenders arrested for stimulant-related crimes		9,868	8,584	8,471
	Boryokudan gangsters, etc.	4,645	3,738	3,577
	Ratio (%)	47.1%	43.5%	42.2%
	Foreigners	632	761	480
	Ratio (%)	6.4%	8.9%	5.7%
Offenders arrested for cannabis-related crimes		3,578	4,321	5,034
	Boryokudan gangsters, etc.	762	780	751
	Ratio (%)	21.3%	18.1%	14.9%
	Foreigners	253	279	292
	Ratio (%)	7.1%	6.5%	5.8%

(b) Modus operandi of money laundering

Regarding the modus operandi of money laundering offenses related to narcotics-related crimes, there have been many cases where proceeds were transferred to accounts under the name of other parties to conceal the proceeds such as:

- A case where traffickers of stimulants by hand delivery or mail had payments transferred to an account under the name of another person
- A case where traffickers of cannabis, etc. by using door-to-door delivery services had payments transferred to an account under the name of another person

There has also been a case where suspicious fund transfers (suspicious transfers of drug payments into a bank account) involving a bank account under the name of a relative of a Boryokudan member led to an investigation that cleared a case of stimulant smuggling following the investigation of the Boryokudan member and others

Automobiles, land, buildings, etc. were also targeted for temporary restraining order for confiscation before the offenders were prosecuted based on the previous Anti-Drug Special Provisions Law, and it is recognized that the criminal proceeds, etc. obtained as cash, etc. have changed in form.

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

We analyzed cleared cases of money laundering (3 years from 2018 to 2020) and counted the detected transactions, etc. to be misused for money laundering while conducting criminal investigations[*1].

There were 420 cases of domestic exchange transactions[*2], 293 cases of cash transactions and 169 cases of deposit transactions that were misused of money laundering. They accounted for the majority of the transactions misused for money laundering (see Table 12).

Table 12 [Major Transactions, etc. Misused for Money Laundering]

Year \ Misused transactions	Domestic exchange transactions	Cash transactions	Deposit transactions	Legal persons	Credit card	International transactions (such as foreign exchanges)	Crypto-assets	Electronic money	Funds transfer services	Precious metals and stones	Postal receiving service	Legal/accounting professionals	Money lending	Note/check	Foreign Currency Exchanges	Total (Number of cases)
2018	150	112	42	15	8	11	1	6	4	0	1	1	0	0	0	351
2019	160	61	31	14	15	14	2	12	6	3	3	1	1	1	0	324
2020	110	120	96	14	20	16	32	12	1	2	0	1	0	0	1	425
Total (Number of cases)	420	293	169	43	43	41	35	30	11	5	4	3	1	1	1	1,100

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)
- ○ Remitting criminal proceeds from fraud to accounts of dummy corporations (Legal persons[*3])
- ○ Remitting criminal proceeds from fraud from a foreign country to an account in Japan (Transactions with a foreign country)

---

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

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

*3 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*.

- Selling gold ingots acquired by theft under the name of a legal person through a friend of the offender (Precious Metals and Stones)
- Receiving criminal proceeds from fraud through a postal receiving service provider (Postal receiving service) and so on.

Cases of misusing those transactions, etc. are individually explained under each part in *Section 5 Risk of Products and Services*.

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 2020 by business type, banks, etc. occupy the largest share, accounting for 74.0% (319,812), followed by credit card companies 6.7% (29,138) and money lending companies 5.8% (25,255) (see Table 13).

The number of STRs used for the investigation, etc. by the prefectural police in 2020 was 325,643 (See Table 14).

Table 13 [Number of Received STRs by Each Business Type]

Category \ Year	2018	2019	2020
	Number of reports	Number of reports	Number of reports
Financial institutions, etc.	401,155	415,299	402,868
Deposit-taking institutions	363,380	366,973	342,226
Banks, etc.	346,014	344,523	319,812
Shinkin Banks, Credit Cooperative	14,375	19,487	19,793
Labour Banks	467	371	300
Norinchukin Banks, etc.	2,524	2,592	2,321
Insurance Companies	2,671	2,876	2,635
Financial Instruments Business Operators	13,345	17,116	17,933
Money Lenders	12,396	17,316	25,255
Fund Transfer Service Providers	1,391	3,913	6,040
Crypto-assets Exchange Service Providers	7,096	5,996	8,023
Commodity Derivatives Business Operators	50	256	320
Currency Exchange Operators	649	712	252
Electronic Monetary Claim Recording Institutions	10	4	5
Others	167	137	179
Financial Leasing Operators	222	270	123
Credit Card Operators	15,114	24,691	29,138
Real Estate Brokers	8	6	7
Dealers in Precious Metals and Stones	952	217	63
Postal Receiving Service Providers	6	4	2
Telephone Receiving Service Providers	0	0	0
Telephone Forwarding Service Providers	8	5	1
Total	417,465	440,492	432,202

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

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

	2018	2019	2020
Number of STRs used in investigation	314,296	307,786	325,643

[Examples of cleared cases using STRs in investigation of initiated cases]

* 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, etc.

(1) Deposit-taking institutions, money lenders, and credit card operators submitted STRs as below, concerning accounts of Japanese people or contract (including those that were declined).

- ○ Opening accounts and applying for loans with forged driver's licenses
- ○ Receiving large amounts of remittances from specific people, followed by subsequent withdrawals
- ○ Suspicion of using fictitious names or other people's names
- ○ Unnatural transaction content in light of the transaction purpose and occupation declared at the time of opening the accounts

With the above as a starting point, it was discovered that some accounts were illegally opened by third parties and used in fraud cases. The users of those accounts were arrested in violation of the Act on Punishment of Organized Crimes (concealment of criminal procedures).

(2) Deposit-taking institutions submitted STRs as below, concerning accounts (including those that were declined) of Japanese people.

- ○ Frequent remittances from a large number of people, followed by subsequent withdrawals
- ○ Sudden large deposits and withdrawals
- ○ Listed as frozen account holders
- ○ Transactions related to Boryokudan and Boryokudan-associated members

With the above as a starting point, it was discovered that some accounts were used by loan sharks as accounts opened under borrowed names. The users of such accounts were arrested in violation of the Money Lending Business Act (unregistered business operation) and the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

2. Fraud Cases

(1) Financial instruments business operators, money lenders, and crypto-asset exchange service providers submitted STRs as below, concerning accounts of Japanese people or contracts (including those that were declined).

- ○ Declaration of a large amount of financial assets by a young account holder
- ○ Unnatural transaction content in light of the occupation declared at the time of opening the accounts
- ○ Suspicion of illegal transfer of crypto-assets by impersonation
- ○ Login from multiple places at nearly the same time, which is temporally and physically impossible
- ○ Suspicion of using fictitious names or other people's names
- ○ Transactions by name lending
- ○ Report on fraud by the account holder

With the above as a starting point, it was discovered that users of the account illegally received public funds, and such users were arrested for fraud.

(2) Deposit-taking institutions, financial instruments business operators, and credit card companies submitted STRs as below, concerning accounts of Japanese people or contracts (including those that were declined).

- ○ Sudden large amounts of deposits, followed by frequent onward remittances
- ○ Suspicious remittances in another name
- ○ Economically unreasonable large amounts of remittances from other countries
- ○ Unnatural transaction content in light of the transaction purpose and occupation declared at the time of opening the accounts
- ○ Fund transfer, either directly or through multiple accounts, to an account related to an account suspected of illegal use
- ○ Use of multiple accounts under the name of other parties by the same person, which is confirmed with a security camera that shows the ATM, etc.

With the above as a starting point, it was discovered that several people, including the account holder, obtained cash by fraud in the name of acquiring funds for a fictitious company. The account holder and others were arrested for fraud.

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

Deposit-taking institutions, credit card operators. and insurance companies submitted STRs as below, concerning accounts of Japanese people or contract (including those that were declined).

- ○ Sudden large deposits and withdrawals
- ○ Depositing money, followed by repeated withdrawals of cash from ATMs installed at convenience stores or another bank
- ○ Frequent remittances from many individuals, followed by the withdrawal of all amount on the same day
- ○ Listed as frozen account holders
- ○ Transactions related to Boryokudan and Boryokudan-associated members

With the above as a starting point, it was discovered that the accounts were used for loan shark offenses. Several related parties, including the account holders, were arrested in violation of the Investment Act (high interest rates) and the Money Lending Business Act (unregistered business operation).

4. Case of Violation of the Immigration Control and Refugee Recognition Act

(1) Deposit-taking institutions submitted STRs as below, concerning accounts of Japanese people and companies (including those that were declined).

- ○ No documents for reviewing the actual status of business were presented when opening an account
- ○ Frequent deposits and withdrawals of large amounts of cash
- ○ A large amount of cash withdrawal or a small amount of transfer to many people, which is funded by a large amount of cash deposit in the name of payment of living expenses
- ○ No document, etc. for remittance was presented during consultation about overseas remittance in the name of education funds by a foreigner in Japan
- ○ Receiving a request from an account under the name of an individual even though transactions are carried out by companies, which is unnatural compared to general transactions

With the above as a starting point, it was discovered that the account holder forced foreigners to engage in illegal work and the people involved were engaged in unauthorized activities. They were arrested in violation of the Immigration Control Act (illegal employment promotion of and unauthorized activities).

(2) A deposit-taking institution submitted STRs as below, concerning a foreigner‘s accounts.

- ○ Large amounts of remittances
- ○ A transaction that deviates from past transaction behavior
- ○ Frequent remittances in a short period of time, in which almost the same amount was deposited and withdrawn in a certain period
- ○ Frequent remittances from an unspecified large number of foreigners to an account belonging to a student, and remittances to a specific company

With the above as a starting point, it was discovered that the account holder had a forged residence card and was arrested in violation of the Immigration Control Act (possession of a forged residence card).

5. Narcotics-related crimes

(1) Deposit-taking institutions and fund transfer business operators submitted STRs as the following reasons, etc., concerning accounts of Japanese people or contract (including those that were declined).

- ○ Transfers from multiple individuals, followed by occasional fund transfers to accounts at other banks
- ○ Suspicious remittances in another name
- ○ Frequent transfers from multiple people, followed by subsequent withdrawals
- ○ Listed as frozen account holders
- ○ Transactions related to Boryokudan and Boryokudan-associated members

With the above as a starting point, suspicious fund transfers related to the accounts were found. The people involved (Boryokudan member, etc.) and the account holder (Boryokudan member) were arrested in violation of the Stimulants Control Act (Act No. 252 of 1951) (joint use).

(2) A deposit-taking institution submitted STRs as the following reasons, etc., concerning accounts of Japanese people.

- ○ Frequent transfers from multiple individuals
- ○ Withdrawals from ATMs installed at convenience stores that are located far from the registered address of an account holder or at another bank
- ○ Use of the same terminal number and IP address for online banking as those used for another account suspected of illegal use
- ○ No reasonable explanation by a customer upon confirmation
- ○ Use of multiple accounts with different account holder names by the same person, which was confirmed with a security camera that shows the ATM, etc.
- ○ Transactions related to Boryokudan and Boryokudan-associated members

With the above as a starting point, suspicious fund transfers related to the accounts were found. The people involved, including the users of the accounts, were arrested in violation of the Stimulants Control Act (transfer for commercial purpose, etc.) and the Anti-drug Special Provisions Law (transfer as business).

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

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

- ○ Sudden large deposits and withdrawals
- ○ A transaction that deviates from past transaction behavior
- ○ Unnatural transaction content in light of the transaction purpose and occupation declared at the time of opening the accounts
- ○ Frequent remittances in a short period

- ○ Suspicious remittances in another name
- ○ Almost the same amount of deposits and withdrawals were made in a certain period
- ○ Frequent transfers from an unspecified large number of individuals, followed by withdrawals of most of the amount transferred

With the above as a starting point, the suspicious fund transfers related to the account was found. The account holder was arrested in violation of the Banking Act (unlicensed banking business).

7. Cases of Fraud and Violating the Act on Prevention of Transfer of Criminal Proceeds

(1) Deposit-taking institutions, money lenders, and insurance companies submitted STRs as the following reasons, etc., concerning accounts of Japanese people or contract (including those that were declined).

- ○ Frequent remittances to many people
- ○ Large amounts of withdrawals from ATMs
- ○ Frequent remittances in a short period of time, in which almost the same amount is deposited and withdrawn in a certain period
- ○ Large amounts of cash transactions
- ○ Transactions related to Boryokudan and Boryokudan-associated members

With the above as a starting point, it turned out that the account holders had opened the accounts with the secret that they were Boryokudan members, and they were arrested for fraud.

(2) Deposit-taking institutions, money lenders, and crypto-asset exchange service providers submitted STRs as the following reasons, etc., concerning accounts of Japanese people or contract (including those that were declined).

- ○ Suspicion of using fictitious names or other people's names
- ○ Transfers from an unspecified large number of people, followed by subsequent cash withdrawals
- ○ Remittances from a place far from an account holder's registered address to an account, followed by the purchase of crypto-assets and remittances
- ○ Being unable to reach an account holder at the provided telephone number and not receiving any response to notifications
- ○ Listed as frozen account holders

With the above as a starting point, it was discovered that some accounts were used by a third party other than the account holders. The account holders were arrested for computer fraud, in which an account was opened for the purpose of assigning it to someone else, and in violation of the Act on Prevention of Transfer of Criminal Proceeds (transfer of passbooks, etc.), in which the offenders assigned an account to a third party. Some accounts were used for specialized fraud.

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

A. Factors that Increase Risks

(a) Characteristics

Non-face-to-face transactions via the Internet, etc. have been increasing due to the development of information communications technologies, improvement in services by 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 misusing non-face-to-face transactions for money laundering:

- An offender opened an account under the name of another person through a non-face-to-face transaction via the Internet by using an identification document, such as a stolen health insurance card, and misused the account to conceal criminal proceeds obtained from selling stolen goods.
- An offender opened an account through a non-face-to-face transaction via the Internet by impersonating a fictious person and misused the account to conceal criminal proceeds obtained from fraud and loan shark offenses.
- An offender designated multiple accounts under fictitious names opened through non-face-to-face transactions via the Internet with forged identification documents as accounts for receiving payments in online banking fraud
- An offender transferred criminal proceeds obtained from fraud offenses to a bank account opened through a non-face-to-face transaction via the Internet (using a smartphone app) by using an identification document with a photo during the long absence of a relative.
- An offender received a cash card by applying to open a bank account through a non-face-to-face transaction via the Internet with a forged health insurance card and presenting the forged card used when opening the account to a postal worker when the cash card was sent by restricted mail.

- An offender opened an account under the name of a fictious company through a non-face-to-face transaction via the Internet to transfer criminal proceeds obtained from special fraud offenses to the account.
- An offender applied to open a bank account under the name of another person and applied for a money lending contract by using the image of a forged driver's license of another person , then transferred the loan money to the account.
- An offender entered into a credit card loan agreement to borrow money from online banking through a non-face-to-face transaction via the Internet by using the illegally obtained bank account information of another account holder and pretending to be that person and transferred criminal proceeds obtained from fraud to an account managed by the offender.

B. Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds and the Ordinance stipulates measures for customer identification that specified business operators need to take when customers' identification documents are not presented to them directly. These measures include sending documents related to transactions by registered mail, etc. that requires no forwarding mail, etc. or by restricted mail.

However, in recent years, illegal cases have been seen relating to customer identification where transaction documents are sent by mail that requires no forwarding and by certified mail with the delivery restricted to the addressee. In those cases, the offender declared an unoccupied address as their address by using copies of forged identification documents and received the transaction documents, such as cash cards and credit cards, delivered to the relevant unoccupied residences. In light of this situation, the Order for Partially Amending the Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds (2018 Ministerial Ordinance No. 3 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, and hereinafter referred to as the "Amendment Ordinance") for establishing measures to mitigate risks was promulgated in November 2018 and enforced in April 2020.

The following is an overview of the revision:

- The Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds used to require one type of identification documents or a copy to be sent in order to verify the identity when sending documents related to transactions by registered mail, etc. that requires no forwarding mail, etc. However, the amended Act requires two types of identification documents, or one type of identification documents plus supplemental documents containing the current addresses of customers or a copy thereof, to be sent when a copy of identification documents is sent.
- The previous Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds stipulates that identification documents with or without photo can be used to verify the customer's identity for documents related to transactions sent as restricted mail. However, the Amendment Ordinance stipulates that only identification documents with photo can be used.

The Amendment Ordinance, in which a system for completing the identity verification online is established to respond to FinTech, was enacted on the date of promulgation.

The following is an overview of the revision:

(i) The Act stipulates methods for having customers take photographs of their appearance using software provided by specified business operators and receiving such images and other images and the like for identification documents with face photos sent by the customers.

(ii) The Ordinance for Enforcement of the Act stipulates the method for receiving images of identification documents (limited to those issued as single documents) with photographs that specified business operators required the customers to take using software provided by them, using customer identification records verified by other specified business operators, and transferring money to the customers' savings accounts (limited to those for which the customer identification data of customers, etc. has been verified and such records are saved), and receiving copies of deposit passbooks, etc. indicating the amount of transferred money sent by the customers.

Measures have been taken for these systems in order to mitigate assumed risks, such as the impersonation of a fictional character or third party by using the images of a third party taken by a customer in advance or by using processed images.

For example, use of processed data is prevented by allowing only software developed by specified business operators or other software developed by a third party and licensed to specified business operators to be used to take and send images in (i) and (ii) above. Specified business operators are required to use appropriate software that will not negatively affect the accuracy of customer identification due to processing of the data being used. In addition, the identification documents usable for (i) and (ii) above are limited to identification documents with photographs. Furthermore, other specified business operators stipulated in (ii) above are limited to those who have a continuous transaction relationship with the customers, and to deposit-taking institutions and credit card operators with necessary technology platforms that are maintained in relatively good condition.

These measures enable efficient customer identification to be completed online while maintaining the standards for customer identification properly.

In addition, the Financial Services Agency's Guidelines for Supervision provides that one area of focus for supervision is whether financial institutions have developed a system necessary to conduct verification at the time of transaction, including CDD measures based on the fact that Internet banking is a non-face-to-face transaction.

Specified business operators are also implementing measures to mitigate risk such as monitoring transactions based on the IP address and login address when judging whether transactions are suspicious.

C. 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

A. 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 15). Use of cash in Japan is higher than that in other countries (see Table 16).

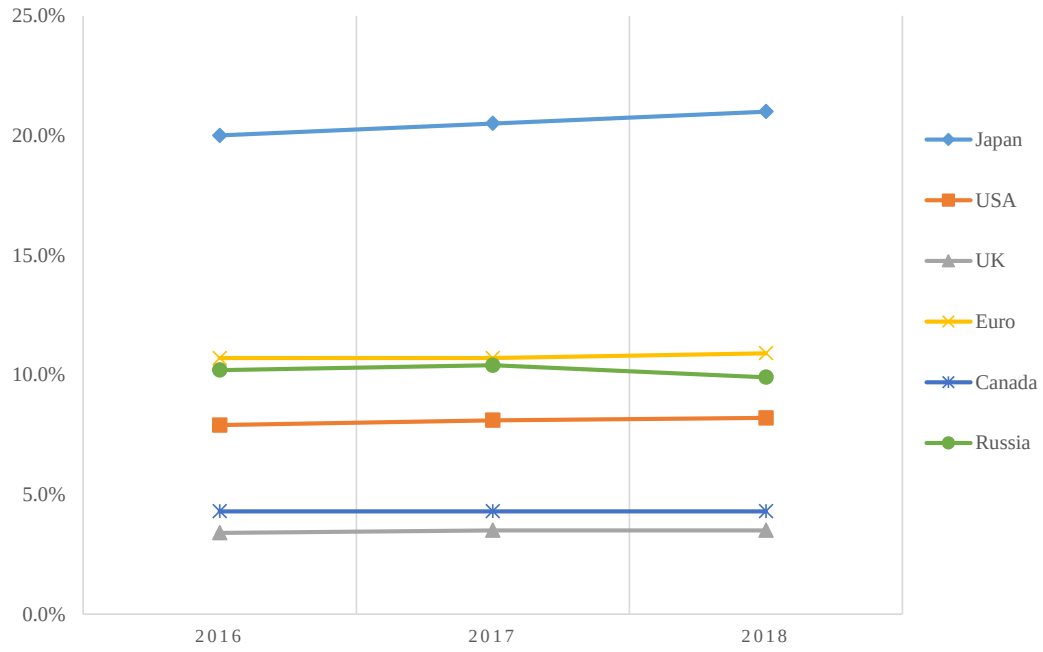
While a reasonable time is necessary for cash transactions because cash is physically transferred, cash transactions are highly anonymous, which is different from foreign/domestic exchange transactions where funds can be transferred to remote locations promptly. Cash transactions are unique in that the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

Table 15 [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 16 [Ratio of Cash Distribution Balance for Different Countries in Nominal GDP]



Note: By BIS Statistics Explorer

(b) Typologies

Through analyzing cleared cases of money laundering, we found that in Japan, there are many cases where those who plan to conduct money laundering have their victims make payment to bank accounts opened in the name of fictitious or other parties through domestic exchange transactions and finally withdraw the money from an ATM, which makes it difficult to trace the funds thereafter. We also found that crime organizations, etc. conceal criminal proceeds in cash. There have been cases where large amounts of criminal proceeds from gambling or loan shark offenses, etc. concealed in cash in safes managed by criminal organizations were confiscated.

There was another case of an international money laundering offense where an international criminal organization remitted the criminal proceeds from fraud committed overseas to a financial institution in Japan and withdrew a large amount of cash in one lump sum, disguising it as a legitimate transaction.

Using cash couriers (physical cross-border transportation of cash and other means of payment) is another way to transfer criminal proceeds across borders. There was a case where an attempt to illegally export a large amount of cash that was criminal proceeds obtained through smuggling gold bullion without permission from the Director-General of Customs was discovered. Another cleared case involved an offender attempting to take criminal proceeds in cash obtained from specialized fraud out of Japan as checked luggage for air travel without declaring it to the Director-General of Customs.

In addition to the above, the following cases are common examples of misusing cash transactions for money laundering:

- Offenders obtained cash by selling or pawning stolen items in the name of a fictitious or another party at secondhand shops, pawnshops, etc.
- Boryokudan members and others received illegal proceeds in cash derived from criminal activities such as prostitution and gambling in the name of protection fees and contributions.

The following are cases where misuse of the liquidity, anonymity, etc. of cash in addition to the vulnerability of products/services provided by the specified business operators to misuse for ML/TF was recognized.

- An offender deposited a large amount of coins obtained by theft into another person's account at an ATM operated by a financial institution, and then withdrew the stolen money in bill at another ATM.
- An offender deposited some of cash obtained through armed robbery into an account multiple times in a short period under the name of his/her acquaintance via an ATM.
- An offender transferred cash derived from the sale of a car obtained from fraud to a foreign country using a fund transfer service provider.
- An offender withdrew cash from a bank account to which criminal proceeds from specialized fraud were transferred, remitted the money to the account of a crypto-assets exchange service provider opened at an Internet bank to purchase crypto-assets, and then transferred it to multiple accounts.

B. 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, anybody who wishes to export or import cash, etc. equivalent to over 1 million yen (100,000 yen if the export destination is North Korea) in person must submit a written declaration to the Finance Minister under the Foreign Exchange and Foreign Trade Act and to the Director-General of Customs under the Customs Act (Act No. 61 of 1954), which are considered to be measures that contribute to reducing the 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.

Furthermore, competent authorities are providing specified business operators with the List of Reference Cases of Suspicious Transactions, etc. which shows examples of potentially suspicious transactions to which specified business operators should pay special attention. The list illustrates cases focusing on cash usage, such as:

- Transactions involving large amounts of cash
- Frequent transactions in a short period, made in large amounts,

and so on.

In light of the above examples, specified business operators take the following measures to mitigate risks:

- 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.

C. 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

A. Factors that Increase Risks

(a) Characteristics

In 2020, Japan's economy was the third largest in the world in terms of nominal GDP (approximately 538.7 trillion yen), the fourth largest in terms of overall import value (approximately 67.8371 trillion yen, and the fifth largest in terms of overall export value (approximately 68.4005 trillion yen). Japan also has a highly advanced financial market, which is one of the leading international financial markets around the world, an enormous number of transactions are conducted.

As indicated above, Japan routinely conducts transactions with other countries. Compared with domestic transactions, international transactions, by their very nature, may generally make it difficult to track funds due 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 directors 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 misused to conceal criminal proceeds. Also, passing through more than one such high-anonymity legal person's account will increase risk as the final transfer destination become unclear. Furthermore, disguising remittances as payments for foreign trade makes it easy to justify them, 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 in a short time, according to correspondent contracts[*1] between banks. This may significantly hinder the tracing of criminal proceeds.

In addition, 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.

Recent years have also seen cross-border money laundering offenses by international criminal organizations 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, cash couriers may be misused for ML/TF 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 measures. In light of these circumstances, financial institutions engaging in foreign-exchange transactions are required to respond while duly considering overseas trends, such as supervisory oversight by domestic and foreign authorities.

(b) Typologies

In recent years, involvement of visiting foreigners has been recognized in many cases of misusing international transactions for money laundering in Japan.

Looking at the status of cleared cases of money laundering committed by foreigners in Japan by nationality, the ratio of Chinese and Vietnamese was high; and looking at it by predicate offenses, the ratio of fraud, theft, violation of the Immigration Control Act, and computer fraud was high. With respect to money laundering cases committed by foreigners in Japan, *Section 3. Analysis of Money Laundering Cases, etc.* of this NRA-FUR explains the results of the survey and provides analysis.

---

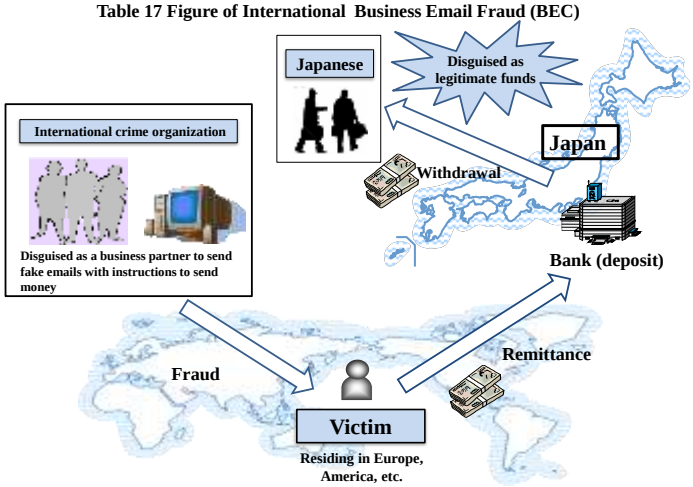
*1 Contracts for continuous or repeated exchange transactions with exchange transaction business operators located in foreign countries.

In terms of the number of STRs related to foreign remittances between 2018 and 2020, reports on remittances to/from China, Hong Kong, and the U.S. occupy about half the total number of STRs. The number of reports on Nepal, Cambodia, Vietnam, and other Asian countries is increasing.

There are international money laundering cases in which international crime organizations use the accounts of financial institutions in Japan to deposit money stolen by fraud committed in foreign countries, and accomplices in Japan withdraw the money by pretending to receive remittances from legal transactions. The following cases are examples of international money laundering:

- 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.

Table 17 Figure of International Business Email Fraud (BEC)



- An offender hacked a server, pretended to be a transaction counterparty to a foreign company, sent an email falsely notifying the company of a change in the destination of a remittance payment, deceived the company into remitting the payment to an account opened in the name of a shell company, and then withdrew a large amount of cash in one lump sum.

The following are the main characteristics of these money laundering cases where the true source of funds and their actual status are concealed by disguising criminal proceeds from fraud committed overseas as legitimate funds:

- 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 addition to the above, there have been cases where an offender opened an account at a financial institution's branch that is located far from the head office in advance by lying about the purpose for opening the account in order to conceal criminal proceeds transferred from overseas.

The following cases are examples of offenses disguised as legal trade:

- A case where the beneficial manager of a company exporting used cars, etc. prepared false documents for stolen cars and exported them abroad using export permits obtained based on false information.
- A case where a used car, etc. that was in high demand in foreign countries was purchased after receiving a remittance request from a customer. The car, etc. was exported in a deal disguised as a legitimate transaction, and subsequently converted to cash. This arrangement was in effect equivalent to an international remittance.
- A case where money remitted by a customer to an account opened in another person's name was used to purchase heavy machinery and agricultural equipment, with the purchased machinery and equipment exported abroad in a deal disguised as a legitimate transaction, and subsequently converted to cash there. This arrangement was in effect equivalent to an international remittance
- A case where money remitted by a customer to an account opened in a foreigner's name was withdrawn in cash and given to a company managed by a foreigner in Japan. The company exported Japanese products purchased with the cash and sold them locally. This arrangement was in effect equivalent to an international remittance.

As described above, the criminal proceeds were turned from cash into goods and to cash again. The modus operandi for offenses has grown sophisticated.

In addition, we found cases where a crime group consisting of a study abroad service agent in a foreign country and foreigners who conspired with the agent operated a large-scale underground bank by using the accounts, etc. managed by the group in and outside Japan without actually transferring funds in order to provide remittance and payment services for families of foreign students back in their home countries; and cases where foreigners illegally staying in Japan used an underground bank to send criminal proceeds, etc. overseas as an underground bank offense case. Although the number of cleared cases has been decreasing since 2014, it is necessary to pay attention to the modus operandi related to underground bank offense cases. For example, there has been a cleared organized offense case involving illegal remittance exceeding two billion yen. It cannot be denied that criminal proceeds from fraud, drug-related, and other offenses may be illegally transferred overseas by underground banks.

Examples of the import and export of a large amount of cash, etc. by personally taking it out include cases where an offender forced a customer to make a remittance request and transfer money to an account under the name of another person and smuggle withdrawn cash by carrying it in a travel bag, etc. into a foreign country. In foreign countries, there have been cases of cross-border bulk cash smuggling and cases where criminal proceeds were transferred overseas by paying more than the actual price of goods, etc.

B. 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, the Supervision Guidelines established by the Financial Services Agency stipulate that the following points shall be considered when supervising the execution of correspondent contracts.

- Proper examination and judgment of the conclusion and continuation of correspondent banking relationships, including approval by supervisory compliance officers after collecting sufficient information about AML/CFT measures by respondent institutions and supervisory measures by the local authorities, etc.;
- To clarify the allocation of responsibility for preventing ML/TF with respondent institutions, by documentation, etc.; and
- To verify that respondent institutions are not shell banks and the institutions do not allow shell banks to use accounts.

Furthermore, when a cash courier imports or exports means of payment exceeding an amount equivalent to 1 million yen in cash (100,000 yen if the export destination is North Korea), checks, and securities, etc. or over 1 kg of precious metals[*2] to be imported or exported by hand, the person is obliged to submit a written declaration to the Finance Minister under the Foreign Exchange and Foreign Trade Act and to the Director-General of Customs under the Customs Act.

The Ministry of Finance has improved the Foreign Exchange Inspection Manual, which highlights focal points related to the development of internal control systems regarding CDD, including verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds. In September 2018, the Ministry formulated the Foreign Exchange Inspection Guidelines, which explain in detail specific inspection items related to developing a system necessary for financial institutions to voluntarily and proactively promote the observance of the Foreign Exchange Act, etc. in light of the risk-based approach.

---

*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.

Furthermore, the Financial Services Agency has been strengthening its supervisory initiatives with a focus on remittance transactions, such as overseas remittances. Activities include conducting a survey of deposit-taking institutions and funds transfer service providers on remittance transactions, etc.

Specified business operators are also taking measures to mitigate risk, including those specified below.

- 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
- 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 by focusing on the discrepancy between the purpose of remittances from foreign countries and the recipients' usage of funds

C. 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 FATF Recommendations and its Interpretive Notes, 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.

[Money Laundering Related to Transactions of Illegal Wild Life Trade]

In the report[*1] published in June 2020, the FATF showed its concern about illegal wildlife trades. They are cross-border organized crimes that generate criminal proceeds of several billion dollars each year, promote corruption, threaten the biodiversity, and have a material impact on public health and economy.

The G7 2030 Nature Compact[*2], an agreement reached at the G7 Cornwall Summit held in the U.K. in June 2021, also includes provisions for designating transactions of illegal wild life trade as a serious organized crime, identifying and assessing the risk of money laundering and enforcing countermeasures.

Although there has been no case of transactions of illegal wild life trade cleared over money laundering in Japan, the following cases are examples of cleared cases in recent years related to the smuggling of wild fauna and flora in Japan.

- A case where an offender imported a living small Asian clawed otter hidden in an overnight bag from Thailand without the necessary approval or permit
- A case where an offender tried to export ivories hidden in suitcases to Laos without the necessary permit
- A case where an offender advertised the sales of materials for making signature stamps using ivories on an internet auction site without the necessary registration

The following cases are examples of money laundering cases related to transactions of illegal wild life trade in foreign counties, which are described in the above FATF report.

- A case where a criminal organization that poaches horns of rhinos in South Africa mainly used cash as the payment method to purchase real estate and luxury cars
- A case where an offender engaging in illegal transactions of armadillos in Indonesia purchased jewelries and other expensive goods after transferring criminal proceeds to the accounts of several relatives

In addition to the above, the report introduced a case where an offender established a shell company to smuggle ivories disguised as legal trade and a case where an offender used electronic payment services for cross-border remittances.

*1 Money Laundering and the Illegal Wildlife Trade (June 2020)

*2 See website of Ministry of Foreign Affairs (https://www.mofa.go.jp/mofaj/ecm/ec/page4_005342.html)

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 Note 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 line with the FATF Recommendations (Recommendation 19), in October 2019 the FATF asked its members to strengthen their oversight of branches and subsidiaries of financial institutions based in Iran to introduce a reporting system or systematic reporting pertaining to Iran-related transactions, and requested that all financial groups toughen their external audits of all branches and subsidiaries situated 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

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.

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 two million yen, in addition to the verification of identification data.

(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 October, 2021[*1]. Even so,

*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, business operators should continue paying attention to the latest statement.

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

[Trends in designated countries/regions from FATF's monitoring process to improve observance of FATF statements and AML/CFT measures]

The following list shows when decisions were made and announced over the last three years (2019 to 2021) regarding the designation of countries/regions targeted for the FATF's monitoring process to improve observance of FATF statements and AML/CFT measures.
Note that the countries/regions announced during the FATF's general meeting in October 2021 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; ◎ indicates that the FATF asked its members and other jurisdictions to conduct enhanced customer due diligence; ▲ indicates that the FATF asked its members and other jurisdictions to conduct enhanced customer due diligence and for financial institutions to tighten their supervision of branches and subsidiaries.

Countries/regions and period	2019			2020			2021		
	Feb.	Jun.	Oct.	Feb.	Jun.	Oct.	Feb.	Jun.	Oct.
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	2019			2020			2021		
	Feb.	Jun.	Oct.	Feb.	Jun.	Oct.	Feb.	Jun.	Oct.
Albania				○	○	○	○	○	○
Barbados				○	○	○	○	○	○
Burkina Faso							○	○	○
Cambodia	○	○	○	○	○	○	○	○	○
Cayman Islands							○	○	○
Haiti								○	○
Jamaica				○	○	○	○	○	○
Jordan									○
Mali									○
Malta								○	○
Morocco							○	○	○
Myanmar				○	○	○	○	○	○
Nicaragua				○	○	○	○	○	○
Pakistan	○	○	○	○	○	○	○	○	○
Panama		○	○	○	○	○	○	○	○
Philippines								○	○
Senegal							○	○	○
South Sudan								○	○
Syria	○	○	○	○	○	○	○	○	○
Turkey									○
Uganda				○	○	○	○	○	○
Yemen	○	○	○	○	○	○	○	○	○
Zimbabwe			○	○	○	○	○	○	○
Bahama	○	○	○	○	○	○			
Botswana	○	○	○	○	○	○	○	○	
Ethiopia	○	○							
Ghana	○	○	○	○	○	○	○		
Iceland			○	○	○				
Mauritius				○	○	○	○	○	
Mongolia			○	○	○				
Serbia	○								
Sri Lanka	○	○							
Trinidad and Tobago	○	○	○						
Tunisia	○	○							

* For the situation in each country, refer to the original text of the statement, Jurisdictions under Increased Monitoring-October 2021 (https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2021.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 FATF's 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.)

A. Factors that Increase Risks

(a) Characteristics

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, 2021, 24 groups are listed as designated Boryokudan under the Act on Prevention of Unjust Acts by Organized Crime Group Members.

At the end of 2020, the total number of Boryokudan gangsters was 25,900[*3] including 13,300 Boryokudan members and 12,700 associates. 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.

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, specialized fraud, fraud misusing public benefit programs, and smuggling of gold bullions. In 2020, there were new fund-raising offenses, including the illegal receipt of benefits related to COVID-19. Moreover, Boryokudan commit

---

*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.

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

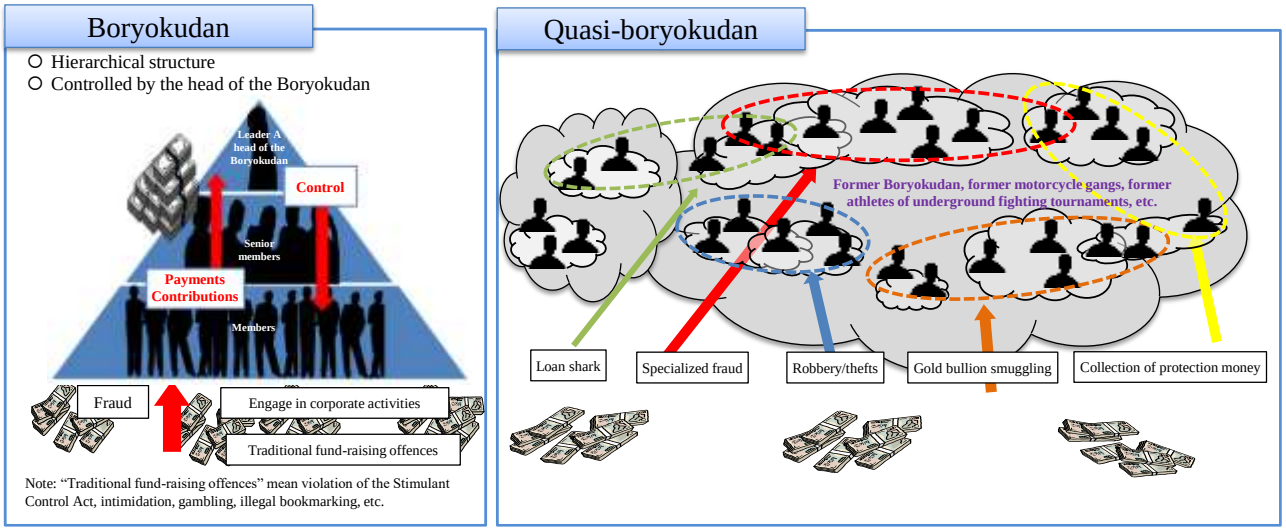
crimes such as offenses under the Money Lending Business Act, the Worker Dispatching Act, etc. to obtain funds, disguising their activities as general economic transactions by using Boryokudan-affiliated companies which are substantially involved in their management or colluding with persons who cooperate with or assist in the money-making activities[*1], etc. of Boryokudan to conceal their actual state, and their funding activities have become more crafted. It is increasingly difficult to define them. Boryokudan often conducts money laundering to avoid 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.

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 their organizational structure is not as clear as those of Boryokudan (hereinafter referred to as "quasi-Boryokudan") engaging themselves in violent, illegal acts habitually. They have been conducting illegal funding activities, such as specialized fraud 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.

Furthermore, quasi-Boryokudan members commit illegal acts, such as specialized fraud, 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.

Boryokudan and quasi-Boryokudan members collude while evading regulations, such as the Anti-Boryokudan Act and Organized Crime Exclusion Ordinances. It can be seen that the funds are being obtained skillfully. Therefore, to accurately grasp the actual situation of these fund-raising activities, a comprehensive response through public-private partnership is required.

Table 18 [Characteristics of Boryokudan and Quasi-Boryokudan]



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

(b) Typologies

There were 1,648 cleared cases of money laundering from 2018 to 2020, including 181 cases (11.0% of total cases) related to Boryokudan gangsters.

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

- Boryokudan concealed ownership of criminal proceeds obtained through fraud, including specialized fraud, illegal money-lending business, drug offenses, offenses against the Worker Dispatching Act, etc., by using an account in the name of another party, etc.
- Boryokudan received criminal proceeds in the name of protection fees, contributions, etc., by taking advantage of their organization's threatening behavior.
- A Boryokudan member knowingly received criminal proceeds generated from prostitution transferred to an account in the name of his/her relative.
- A Boryokudan member sent health foods without needing it by using a cash-on-delivery postal service, having deceived the victim into remitting the proceeds of the sale through the company providing the service to an account opened by the offender's acquaintance under the name of a dummy corporation.
- A Boryokudan member used an account opened by his wife under her maiden name as a repayment account for a loan shark.
- A Boryokudan member knowingly received criminal proceeds from specialized fraud by registered mail.

The following cases are the examples of quasi-Boryokudan's fund-raising activities.

- Quasi-Boryokudan-related members acted as lawyers and stole cash by deceiving elderly people in the name of avoiding proceedings related to troubles.
- Quasi-Boryokudan-related members acted as trading company employees and stole cash by deceiving elderly people to solve problems related to name lending for use in purchasing bonds.
- Quasi-Boryokudan-related members pretended to be real estate-related company employees, offered false acquisition stories to landowners, and stole cash by deceiving them in the name of expenses related to land sales contracts.

B Trends of STRs

There were 1,290,159 STRs from 2018 to 2020, including 172,724 reports (13.4% of total reports) related to Boryokudan gangsters.

C. 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.

D. 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)

The current international terrorism issues remain severe, with terrorist attacks occurring in various countries including Europe and the U.S. etc. Also, there is a concern that foreign fighters who participated in battles in Iraq and Syria may commit 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.

A. 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 completely 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 attacking. 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, it was announced that he had died in a US operation. On the 31st of the same month, ISIL announced a new leader.

In retaliation against military intervention in Iraq and Syria, ISIL has been continuing to conduct terrorist attacks in countries such as the U.S. and European countries etc. participating in the Global Coalition to Counter ISIL. For 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 from 2020, ISIL continued to plan terrorist attacks against Western and other countries, participating the Global Coalition to Defeat ISIL. Meanwhile, there have been terrorist attacks that are considered to have been affected by the extremism of ISIL, etc. It is indicated that many terrorist attacks that are planned in advance are to occur after the restriction on movement to prevent the spread of COVID-19 is eased.

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 third countries. While the movement of people is limited due to the spread of COVID-19, some of the remaining foreign fighters are still kept in temporary shelters or refugee camps. ISIL has repeatedly urged members and sympathizers to rescue such fighters. In addition, there have been riots by the fighters in temporary shelters who are concerned about the spread of COVID-19, so the vulnerability of temporary shelters for fighters in Syria has been raised.

As for AQ and associated organizations, its leader, Ayman al-Zawahiri, repeatedly advocates for anti-Americanism and anti-Israelism, and urges members and sympathizers to carry out terrorist attacks against Western countries through online bulletin etc. In December 2019, a flight trainee of the Saudi Air Force, who has been communicating with AQAP[*1] for a long time, carried out a terrorist shooting attack in a U.S. military base located in the U.S. where he was dispatched for training.

Also, as AQ-related organizations operating in the Middle East and Africa regions, etc. have been committing terrorism targeting at local government organizations and the like, AQ and its related organizations are still a threat.

It is worth of seeing whether the completion of the withdrawal of the U.S. military from Afghanistan at the end of August 2021 will stimulate the Islamic extremism, which considers the withdrawal as a victory, and

---

*1 Abbreviation of Al-Qaeda in the Arabian Peninsula which is an organization associated with AQ.

whether changes in terrorism threats will occur in and outside Afghanistan. AQ may boost their activities in Afghanistan, which may become the activity base of terrorist groups, depending on the public safety measures taken by the Taliban and its reactions against ISIL-K[*1] and other terrorist groups.

Table 19 [Number of International Terrorism Cases since 2015]

Item/year	2015	2016	2017	2018	2019
Number of cases	11,774	11,072	8,584	8,094	8,302
Number of deaths and injuries	63,648	59,435	38,214	55,487	45,006

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

Table 20 [Major Terrorism Cases in 2020]

Date	Case
March 6	Attack on a Shiite leader's memorial in Kabul, Afghanistan
March 25	Attack on a Sikh house of worship in Kabul, Afghanistan
June 20	Knife attack in Reading, U.K.
August 16	Attack on a hotel in Mogadishu, Somali
August 24	Series of bomb attacks in Jolo Sulu, Philippines
September 25	Knife attack in front of the ex-Charlie Hebdo office in Paris, France
October 16	Knife attack in Conflans Sainte-Honorine, France
October 29	Knife attack in Nice, France
November 2	Terrorism shooting attack in Vienna, Austria

(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 buried and invisible among the numerous transactions handled routinely by business operators.

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

- 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.

The FATF also calls its member countries to prevent nonprofit organizations[*1] 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.

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 Interpretative Notes etc., nonprofit organizations have the following vulnerabilities to terrorist financing:

- 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 about the possibility of transferring funds through non-profit organizations by taking advantage of financial technology including crypto-assets. It is a new fundraising opportunity for terrorists by misusing non-profit organizations.

As for the recent international movement in this context, an initiative on "Ensuring the Implementation of Countering the Financing Terrorism Measures While Safeguarding Civic Space" (tentative name), 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.

Note that 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) 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.

The Cabinet Office investigated the examples of efforts made in foreign countries that require nonprofit organizations to comply with the FATF Recommendations in 2021. Based on the results of the investigation, the Cabinet Office is reviewing the risk assessment of corporation engaging in specified nonprofit activities and them on the risk-based approach.

---

*1 The FATF defines a nonprofit organization as a legal person, legal arrangement, or legal organization that raises and disburses funds for charitable, religious, cultural, educational, social, or mutual aid purpose as the primary goal, or for other acts of charity.

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 Foreign Exchange and Foreign Trade Act and the Act on Special Measures Concerning International Terrorist Assets-Freezing.

○ 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.

- Foreign fighters are recognized as one of the main actors of support for terrorist organizations.
- Technological advances, including social media and new payment methods, have introduced vulnerabilities in terms of terrorist financing.
- In light of the cross-border nature of TF, a jurisdiction that faces a low terrorism risk may still face TF risks. Actors may still exploit vulnerabilities to raise or stole funds or other assets domestically, or to move funds or other assets through the jurisdiction.

○ 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 Case

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 Foreign Exchange Act (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.

○ Self-financing and asking for donations to establish a pro-ISIS group (Singapore)

In 2016, the Singapore authorities arrested a group of self-radicalized Bangladeshi nationals working in Singapore for their involvement in a pro-ISIS group. Six of the Bangladeshi nationals were charged and subsequently convicted for terrorism financing offenses. The group aimed to overthrow the Bangladeshi government and establish an Islamic caliphate in Bangladesh to join ISIS eventually. The

---

*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.

leader of the group solicited donations from its members. The funds were contributions made out of their salaries.

- Funding to develop terrorist recruitment materials (Spain)

  In 2014, several individuals were arrested in Spain on charges of involvement in a recruitment and propaganda scheme for a terrorist organization. The organization was exploiting a fast-food restaurant chain to raise funds for the terrorist organization. The proceeds obtained from the operation of the restaurants were used to create materials for propaganda, including leaflets, books, flags, and videos, which they distributed among the followers that went to the restaurants. During the arrests, officers seized several printers used to reproduce propaganda materials in the back room of the restaurants.

- Use of an individual's own savings to support recruitment (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.

- 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, meeting in various locations in different cities, sometimes using up to three legs to transfer a payment. In one case, an Israeli citizen met up with a person who entered Israel illegally through the Egyptian border and collected USD 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).

- Misuse of Donations (Egypt)

  In 2013, a group of terrorists killed 24 police officers in Egypt. The Egyptian authorities arrested the terrorists who were involved. Afterwards, the investigations revealed that a member of the terrorist group, to which the terrorists belonged, operated a fake charity to raise funds by misusing the name of a well-known charitable organization that is active across the country.

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

On August 28, 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.

B. 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.

C. 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, in light of the risk of virtual currency (crypto-assets) being misused for terrorism financing, which has been pointed out by international organizations, the revised Act on Prevention of Transfer of Criminal Proceeds, under which virtual currency (crypto-assets) exchange service providers have been added as specified business operators, took effect in April 2017.

Moreover, following the amendment of the Act on Punishment of Organized Crimes and Control of Crime Proceeds, which includes a new provision to criminalize the preparation of acts of terrorism and other organized crimes, etc. in June 2017, Japan became a State Party to the United Nations Convention against Transnational Organized Crime, which took effect for Japan on August 10 of the same year.

In addition, each time the National Police Agency updates 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), the competent authorities must ensure that specified business operators 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.

○ Foreign Exchange Act

With respect to international transactions, in response to the United Nations Security Council resolutions (No. 1267 and its succeeding resolutions and No. 1373) on asset freezing and other measures, simultaneous asset freezing by G7 and various other asset-freezing measures have been implemented against individuals and groups subject to such measures in accordance with the Foreign Exchange and Foreign Trade Act. Specifically, as of September 9, 2021, 402 individuals and 120 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 September 9, 2021, the names of 402 individuals and 120 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. In addition, by the amendment of the Order for Enforcement of the International Terrorist Asset-Freezing Act, virtual currency (crypto-assets) was added to the assets which were regulated, for example when gifted to international terrorists, in April 2017.

(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 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

D. 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[*2] 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.

---

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

*2 Terrorist Financing Risk Assessment Guidance (July 2019)

(3) Non-resident Customers

A. Factors that Increase Risks

In the Interpretative Note of 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 customer management measures, including identity verification and verification of assets and income, are more restrictive for non-residents 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.

B. 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.

C. 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

A. 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

B. 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.

C. 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. Also, the FATF Recommendations (e.g., Recommendation 24) 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.

A. 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 or authority over company assets according to their respective positions.

Hence, 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.

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).

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 21).

In the case of a stock company, the articles of incorporation need to be certified by a notary public for the preparation of the articles of incorporation required for the establishment of the corporation. On the other hand, certification of the articles of incorporation by a notary public is not required in the case of a general partnership, a limited partnership, or a limited liability company.

Looking at the number of registered establishments by type of legal person in recent years, the number of establishments of limited liability companies tends to increase (see Table 22).

---

*1 Concealment of Beneficial Ownership (July 2018)

Table 21 [Number of Corporations by Major Corporate Type in Japan]

Category \ Year	2017	2018	2019
Stock company	2,537,667	2,554,582	2,559,561
General partnership companies	3,814	3,371	3,343
Limited partnership companies	16,112	14,170	13,540
Limited liability companies	82,931	98,652	113,196
Others	66,103	67,774	68,780
Total	2,706,627	2,738,549	2,758,420

Note 1: The company sample survey of the National Tax Agency.
2: The number of corporations is the total number of non-consolidated corporations and consolidated corporations.
3: Corporations that are closed or liquidated or general incorporated associations and foundations are excluded.
4: Others refer to cooperative partnerships, special-purpose entities, syndicates, mutual companies, and medical corporations.

Table 22 [Number of Registered Establishments by Each Major Corporate Type]

Category \ Year	2018	2019	2020
Stock company	86,993	87,871	85,688
General partnership companies	87	48	34
Limited partnership companies	52	47	41
Limited liability companies	29,076	30,566	33,236
Total	116,208	118,532	118,999

Note: The statistics of the Ministry of Justice.

Cleared cases of domestic money laundering offenses in which legal persons were misused indicate that people who intend to commit ML/TF by misusing legal persons tend to do so in the following ways:

- Take advantage of trust in transactions
- Frequently transfer large amounts of assets
- Obscure the source of illegal proceeds by mixing criminal proceeds with legitimate business proceeds.

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 2018 to 2020, 43 offenses took advantage of dummy or obscure corporations. Similar offenses have been increasing in number in recent years. Of these, 14 offenses took advantage of dummy or obscure corporations in 2020. The number of corporations abused was 20. Looking at these corporations by type, there were 16 stock companies (including special limited liability companies) and 4 limited liability companies. Comparing the ratio of the number of stock companies and number of limited liabilities companies described in the number of corporations by major type in Japan (see Table 21), it can be seen that the ratio of limited liability companies is higher than that of stock companies.

Furthermore, among the misused legal persons, those that were abused within a noticeably short period after being established were recognized. There were suspicious points that many business purposes were registered by corporations abused, where the relationship between each purpose was low.

In terms of predicate offenses where corporations were abused, fraud accounts for the largest percentage, including fraud committed overseas. Other predicate offenses include violations of the Investment Act, Moneylending Control Act, and Anti-Prostitution Act. We have recognized situations where dummy legal persons or other obscure legal persons have been misused repeatedly and continuously for committed crimes that generate large amounts of money.

Moreover, 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.

In such circumstances 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, and some of them provide incidental services as follows:

- Postal receiving services

  They authorize a customer to use their own address or their office address as the place where the customer receives postal items, then receive postal items addressed to the customer, and deliver those items to the customer.

- Telephone receiving services

  They authorize a customer to use their telephone number as the customer's contact telephone number, then receive telephone calls directed to the customer, and transmit the content to the customer.

- Telephone forwarding services

  They authorize a customer to use their telephone number as the customer's contact telephone number, then automatically forward telephone calls directed to or received from the customer to the telephone number designated by the customer.

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.

(b) Typologies

The following cases are common examples of misusing unclarified legal persons for money laundering:

- A beneficial owner of a company, who established it while putting a third party in place as a representative director, concealed criminal proceeds from fraud in the company's bank account

- A dummy stock company was established by requesting an acquaintance to do so, a bank account was opened in the name of the said stock company, and criminal proceeds from prostitution were concealed in the account as legitimate business proceeds

- Criminal proceeds were remitted to the account of a different dummy company each time and then paid out at the window of a financial institution

- A website was opened in the name of a shell company in order to act as an intermediary for side businesses related to online sales of electronic books. Side businesses using the website were defrauded of money as they were made to remit money in the name of expenditures needed for server upgrades

- An offender used a fictious transaction between fake electronic money traders to obtain the right to use electronic money gift cards obtained from specialized fraud. The offender pretended as if the right to use the gift cards was obtained through a legal transaction and converted them to cash.
- Criminal proceeds from fraud, etc. committed in foreign countries were remitted to an account in the name of a dummy legal person
- An offender caused a third party to transfer part of the cash defrauded from a financial institution as a loan to an illicitly opened account of a company that had no real business operations
- An account in the name of a company of the offender's relative, which had already been dissolved, was used to conceal proceeds obtained by having foreigners engage in illegal work
- Legal person whose actual situation was unclear was established in a tax haven abroad, an account in the name of above legal person was opened at a foreign bank, and criminal proceeds in violation of the Copyright Act were transferred to opened account

The following cases are common examples of misusing criminal proceeds to control business of corporations, etc.:

- An offender obtained the status of a founder by using illegal proceeds obtained from operating a restaurant without license as an investment for obtaining shares for the establishment of a corporation. The offender requested a judicial scrivener, who didn't know that the money was illegally obtained, to register the establishment of the corporation, and designated himself as a representative of the company.

B. Trends of STRs

Looking at the examples of reasons for submitting STRs regarding corporations, it was done because the actual status of the corporation is unclear or its beneficial owner is not identified. STRs focusing on customer attributes, business details, transaction types, etc. were submitted in the following cases:

- The submission of documents, including identification documents, was refused, or the business details or transaction purposes were not explained appropriately.
- It was discovered that a person holding an account related to an officer or corporation is an anti-social force such as Boryokudan.
- An office or store did not exist at the registered address, or a customer could not be reached at the registered telephone number.
- There was an unreasonable number of registered purposes of business, and such purposes were barely related to one another.
- 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 reported business details could not be confirmed, and the balance in the bank account was extremely inappropriate for the business.
- A substantially dormant company had an account in which there were frequent transactions of unclear deposits and withdrawals in cash.
- 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.
- Deposits and remittances in round figures were made to a legal person repeatedly.

C. 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 under the Act on Prevention of Transfer of Criminal Proceeds, Ordinance for Enforcement of the Notary Act (Order of the Attorney-General's Office No. 9 of 1949), Companies Act (Act No. 86 of 2005), etc.

The Act on Prevention of Transfer of Criminal Proceeds and Ordinance require specified business operators to verify the identity of a customer's beneficial owner specified as follows, if the customer is a legal person, etc.

(1): a natural person who directly or indirectly holds more than one-fourth of the voting rights for a legal person to which the principle of capital majority rule applies, such as a stock company[*1];

(2): a natural person who is deemed to have control over the business activities of a legal person to which the principle of capital majority rule applies such as a stock company, in which there is no natural person described in (i) above;

(3): a legal person to which the principle of capital majority rule does not apply and who is (i) a natural person who is deemed to have a right to receive dividends of more than one-fourth of the total amount of revenue arising from the business or distribution of assets in connection with such business[*2] or (ii) a natural person who has control over the business activities of the legal person; and

(4): a legal person in which there is no natural person described in (1) to (3) above and who is a natural person representing the legal person and executing its business.

From the perspective of verifying information on the beneficial owner at the time of establishing a company, the Ordinance for Enforcement of the Notary Act was amended in November 2018 to oblige notaries to report to clients the name of a beneficial owner and whether or not such beneficial owner falls under Boryokudan (a member of an organized crime group)or an international terrorist at the time of certifying the articles of incorporation of stock companies, general incorporated associations or general incorporated foundations.

Furthermore, the Regulation on Storage of Beneficial Ownership Information List in the Commercial Registry Office (Ministry of Justice Public Notice No. 187 of 2021) was established and is scheduled to be enforced in January 2022 to specify that the commercial registry office can store documents containing information on beneficial owners of stock companies at their request, and provide a copy of such documents in order to keep track of the beneficial owners after the establishment of companies.

In addition, 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.

Also, the Companies Act stipulates dissolution of companies deemed to be dormant[*3]. 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 25,000 cases in FY2018, 33,000 cases in FY2019, and 32,000 cases in FY2020.

In addition, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators who provide business addresses, addresses for facilities and means of communication, and administrative addresses for legal persons, etc. to conduct CDD.

D. Assessment of Risks

Legal persons can make the right and controlling interest in their properties complicated. Beneficial owners of legal persons can conceal that they have substantial rights to such properties by making their properties belong to legal persons. Due to this characteristic of a legal person, it is difficult to trace funds owned by legal persons without transparent beneficial owner.

---

*1 Excluding the cases where it is obvious that the relevant natural person does not have intention or ability to substantially control the business management of the relevant legal person to which the principle of capital majority rule applies or where any other natural person directly or indirectly has more than one-half of the voting rights of such legal person to which the principle of capital majority rule applies.

*2 Excluding the cases where it is obvious that the relevant natural person does not have intention or ability to substantially control the business management of the relevant legal person or where any other natural person has the right to receive dividends of proceeds or distribution of assets, which are more than one-half of the total amount of proceeds arising from the business of such legal person or assets related to such business.

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

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.

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]

A. Risk Factors for Deposit-taking Institutions

(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 2021, 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, 652 agricultural cooperatives and fisheries cooperatives, and 60 credit federations of agricultural cooperatives and credit federations of fisheries cooperatives). Among these institutions, banks held a total deposit balance[*3] of 895.6864 trillion yen for a total of 799,090,000 accounts as of the end of March 2021.

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 by a Financial Institution, 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, regional banks II, 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 regional banks II 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 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.).

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

*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.

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 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.

(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. specialized fraud, based on information provided by investigative agencies or others about that account.

b. Typologies

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

- Accounts belonging to deceased persons or foreign nationals who have returned to their home countries without closing their accounts were used to conceal criminal proceeds from fraud, theft, etc.
- Offenders received or concealed criminal proceeds derived from fraud, theft, loan-shark crime, violation of the Amusement Business Act, drug crime, selling fake brand goods, etc., by using accounts sold for the purpose of obtaining money, accounts opened under fictitious names, and accounts opened illegally in the name of shell companies.

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 specialized fraud crimes. Among the cleared cases so far, there were cases where a large number of other people's passbooks and cash cards were seized, including the following case, to be specific.

- Dozens of other people's passbooks and cash cards, most of which belonged to foreigners, were seized from the home of a suspect who belongs to a fraud group arrested for medical expense refund fraud.

Furthermore, although the number of cases of account misuse under corporate names is smaller than the number of cases of account misuse under individual names, there are cases of accounts under corporate

names being misused. For example, accounts under corporate names are misused for crimes committed by organized crime groups that generate large amounts of proceeds, such as specialized fraud or cross-border money laundering offenses.

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 specialized fraud, 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 cases have been cleared. Table 23 shows the number of cases cleared in violation of 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 is necessary to pay attention to the fact that the transfer of accounts encourages the acts of ML/TF. 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 is 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 24).

Table 23 [Number of Cleared Cases of Violating the Act on Prevention of Transfer of Criminal Proceeds]

Category \ Year	2018	2019	2020
Transfer of deposit/savings passbook, etc.	2,519	2,479	2,539
Transfer of deposit/savings passbook, etc. (business)	27	44	18
Solicitation for transfer of deposit/savings passbooks, etc.	27	27	32
Transfer of exchange transaction cards, etc.	0	27	35
Transfer of information for crypto-assets exchange	0	0	6
Others	4	0	4
Total	2,577	2,577	2,634

Table 24 [Number of Cleared Cases of Account Fraud etc.]

Category \ Year	2018	2019	2020
Account fraud	1,277	919	696
Transfer of stolen goods	4	6	7
Total	1,281	925	703

Note: Based on reports on crimes which promote specialized fraud, 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 specialized fraud 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 concealed criminal proceeds derived from theft, fraud, embezzlement, drug crime, gambling, etc., by depositing them 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 senior Boryokudan member received criminal proceeds, which were derived from fraud by an acquaintance, by making the acquaintance remit the proceeds to the member's account.

- An offender made a third party transfer part of the cash obtained from a financial institution in a fraud loan to an illicitly opened account of a company that had no actual business operations.
- An offender took requests from more than one client and had them remit cash for an illegal foreign transfer of money into an account that the offender had purchased from Vietnamese who had returned to their country.
- An offender sold obscene DVDs via a cash-on-delivery postal service and had the delivery service provider remit the received money to an account opened in another person's name.
- Offenders concealed criminal proceeds derived from drug crime, illegal money-lending business, unlicensed adult entertainment shops, etc., by making customers remit to accounts opened in other persons' names.
- A Chinese offender engaging in agriculture in Japan obtained criminal proceeds by forcing a Chinese worker without a work permit to work illegally and remitted the proceeds to an account under the name of a Chinese person whom they had hired before.
- An offender defrauded a victim by specialized fraud and made the victim remit money to an account in another person's name, and then transferred it into an account under their own name that had been opened in advance for the purpose of concealing criminal proceeds.
- A staffing agency made its subsidiary staffing agency remit money to an account under the name of a legal person, knowing that the money is part of the proceeds that the subsidiary agency obtained by dispatching Vietnamese persons without work permits to factories.
- The money obtained from a fraudulent internet auction was transferred to an acquaintance's account in an online bank that had been opened 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 fictious 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 derived from fraud cases were given to a Boryokudan group, and a senior member of the Boryokudan concealed the proceeds in a safe deposit box that had been leased from a bank under the name of a family member.
- 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 bearer checks or checks drawn to self that exceed 2 million yen and are not crossed (in the cases where cash receipt and payment is involved and related to exchange transactions or checks drawn to self, 100,000 yen).

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

b. Typologies

Actual situations exist where persons attempting to commit ML/TF misuse bills and checks as a way to transport the 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).

B. Trends of STRs

The number of STRs submitted by deposit-taking institutions was 1,072,579 between 2018 and 2020, accounting for 83.1% 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 (216,100 reports, 20.2%)
- Transactions related to Boryokudan gangsters or their related parties (143,520 reports, 13.4%)
- 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,

---

*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.

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 (76,411 reports, 7.1%)

- Transactions in which a large amount of money is transferred from foreign countries without an economically justifiable reason (74,192 reports, 6.9%)
- Transactions using accounts that frequently receive remittances from many persons. In particular, cases where money is transferred or paid from the accounts immediately after receiving remittances. (72,504 reports, 6.8%)
- Transactions related to accounts that usually show no movement of funds, but a huge amount of money is suddenly deposited into or withdrawn from them. (68,542 reports, 6.4%)
- Transactions for which a large amount of money is transferred to foreign countries without an economically justifiable reason. (45,572 reports, 4.3%)
- 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. (35,567 reports, 3.3%)
- Transactions related to accounts through which a large amount of money is frequently deposited or withdrawn. (34,079 reports, 3.2%)
- Deposit or withdrawal transactions using accounts suspected to be opened in a fictitious or other person's name. (33,898 reports, 3.2%)

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.

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds imposes the obligation on deposit-taking institutions to conduct verifications at the time of specified transactions when they provide specified products and services, as described above.

Moreover, in addition to supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, the Banking Act states that the Financial Services Agency may require banks to submit reports, conduct on-site inspections of banks, and order banks to make business improvements if necessary. The competent authorities have the right to supervise deposit-taking institutions. In addition, the Comprehensive Guidelines for Supervision by the Financial Services Agency[*1] demands that deposit-taking institutions develop internal control systems to fulfil these obligations[*2].

(b) Measures by competent authorities

The Financial Services Agency released the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in February 2018 to clarify the basic concept of effective AML/CFT measures and to encourage financial institutions to implement effective measures. The Financial Services Agency made the second amendment of the Guidelines in February 2021. Furthermore, for the purpose of improving the understanding of relevant parties on the Guidelines, the Financial Services Agency published an "FAQ Related to the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism." In April of the same year, the Agency urged each financial institution, etc. to establish an effective system for taking AML/CFT measures by requesting them to implement the measures required by the Guidelines by the end of March 2024.

The Financial Services Agency has determined that deposit-taking institutions face relatively higher risks than other types of businesses, taking into account the volume of financial transactions handled by the industry as a whole and globally spreading risks by overseas transfer transactions based on correspondent

---

*1 Regarding the Financial Services Agency's supervision over financial institutions, the Agency produces Comprehensive Guidelines for Supervision that illustrate the notion, viewpoints, important matters, specific methods of supervision, etc.

*2 The Agency requires development of internal control systems, including a system to conduct proper verification at the time of transaction, a system to make proper STRs, a system to conduct integrated and comprehensive management of verification at the time of transaction and STRs, and a system to implement proper AML/CFT measures at overseas business locations.

agreements, etc., and it is focusing its efforts in these areas. Specifically, the Agency is grasping the actual state of compliance with laws and regulations and of risk control by documentary research and by report submission orders, and conducting risk assessment on types of businesses and business operators by gap analysis, etc. between actual status and the Guidelines. Then the Agency provides guidance or supervision, etc. corresponding to risks of business operators based on the assessment results.

Consequently, it is recognized that although many specified business operators prepared the documents ("Risk Assessment Report"), the quality of the documents varies by business operator, furthermore, although risks unique to local financial institutions are not so different from those of major banks, their efforts toward a risk-based approach are still recognized to be quite different from those of major banks. Taking these points into account, the Financial Services Agency requires all deposit-taking institutions, regardless of their size, to implement risk assessments. The Financial Services Agency provides guidance and supervision for their actions towards implementing a risk-based approach, including establishing, maintaining, etc. an internal control system, by not simply focusing on formally checking for any violation of laws and regulations, but also by emphasizing the importance of the relevant laws and regulations, survey reports, and the Guidelines. Together with specialist advisory committees set up by industry associations such as the Japanese Bankers Association, the Financial Services Agency has also been considering issues common to financial institutions, such as the joint operation of a transaction monitoring and filtering system.

Furthermore, the Financial Services Agency continuously provides lectures and trainings to other ministries, industry groups, and financial institutions to improve AML/CFT measures. In 2020, 77 lectures and trainings were given. The Financial Services Agency is working to improve system development at financial institutions nationwide by explaining the purpose of the guideline revision and the main points for conducting ongoing CDD.

The Ministry of Agriculture, Forestry and Fisheries and the Ministry of Health, Labour and Welfare also check documents and issue report submission orders to grasp the actual situation of compliance with laws and regulations and risk control by agricultural cooperatives, labor banks, etc. The Ministries also provide guidance, supervision, etc. corresponding to the risks of respective agricultural cooperatives, labor banks, etc. based on the information obtained through such checks and orders.

The following matters are the main points that deposit-taking institutions should note in light of the actual situation identified by the competent authorities:

- Matters regarding management involvement
  - Management takes initiatives to implement AML/CTF measures and give specific instructions to each relevant department and foster collaboration, etc. among relevant departments, while developing effective risk mitigation measures and action plans. Furthermore, the implementation statuses of the measures are reported regularly and as necessary and discussed if needed.
  - Based on the developed risk mitigation measures and action plans, it is necessary to promote the company-wide measures by understanding the appropriate management resources and reviewing the system, including assigning personnel with expertise and giving a budget.
  - The administrative division must verify the detection statuses of suspicious or abnormal transactions at sales offices and overseas transmittance divisions, and it is necessary to verify the effectiveness of the management system using the risk-based approach.
  - In addition to rules-based internal audits, internal audits using the risk-based approach must be conducted.
- Matters regarding the identification, assessment, etc. of risks
  - In identifying and evaluating risks, the sales department and the management department cooperate and consider the characteristics of individual and specific risks based on the geographical characteristics of one's business area, business environment, management environment, and STR's trends, as well as the results of national risk assessment.
  - When handling new products or services, in addition to the verification of the risks of the products or services, the risk of ML/TF including the effectiveness of a risk management system of business partners, collaborators, contractors and acquired companies, etc. related to the provision of such products or services must be verified before the provision of the products or services.
  - When identifying or assessing the risks related to the loan of funds for import and export transactions or granting credits, etc., it is necessary to consider not only the risks of countries and

regions related to the import and export transactions, but also the risks of the relevant products, contract details, transportation routes, vessels to be used, persons involved in the transactions (including beneficial owners), etc.

- Matters regarding CDD
  - It is necessary to conduct risk assessment of all customers by integrating the results of risk assessment of products, services, transaction types, countries, regions, customer attributes, etc. and to formulate and promote a concrete plan for ongoing CDD such as determining the frequency and method of investigating customer information according to the conducted risk assessment.
  - Information should be shared with sales offices, etc. because some sales offices repeatedly accepted transactions that were similar to those reported as suspicious transactions in the past.
  - Certain measures are being taken to prevent anti-social forces from opening accounts, and to close the accounts that are already open. In addition to such measures, it is important to also monitor and filter transactions, such as remittances carried out by anti-social forces that have existing bank accounts, and consider submitting STRs.
  - When foreigners open accounts, they should be informed that it is a crime to sell accounts to someone else and be reminded to close their accounts when returning to their home countries. In addition, banks should keep track of their periods of stay to detect accounts with deposits and withdrawals even after the periods of stay have expired as a possible case of illegal/unauthorized use of the accounts.
  - When opening an account for a foreigner, if the katakana name and alphabetic name are written on the customer identification documents, the customer attribute of each name should be confirmed.
- Matters regarding Transaction monitoring and transaction filtering
  - For transaction monitoring, it is necessary to set scenarios based on their own ML/TF risks, and consider other risks so that the monitoring targets are not biased towards specific financial crimes, such as specialized fraud cases.
  - Regarding transaction monitoring, it is necessary to set scenarios and threshold values according to customer risk assessments and regularly review the scenarios and threshold values based on a financial crime pattern analysis.
  - It is necessary to establish a system that stores records of overseas remittances as data and can detect, via transaction monitoring, suspicious or abnormal remittances such as those sent by the same remittance requestor to a lot of recipients
  - When persons subject to economic sanctions are designated by a resolution of the United Nations Security Council, etc., such persons should be added to the financial institution's list of persons subject to sanctions within several hours or 24 hours at the latest, and transaction filtering should be conducted to immediately check if there is any difference with the existing customers.
- Matters regarding STRs
  - A system for appropriate examination and judgment should be established for submitting STRs, and the STR status should be used to strengthen the bank's own risk control system.
  - The administrative division must, in addition to distributing the List of Reference Cases of Suspicious Transactions released by the Financial Services Agency to branch offices, communicate to all branch offices specific examples that take into account the risks that they may face, and establish a system that enables them to detect suspicious or abnormal transactions.
- Matters regarding obligations under the Act on Prevention of Transfer of Criminal Proceeds, etc.
  - Conducting the procedures stipulated by law if identification documents without photographs are presented for verification at the time of transaction, by having the customer present or send other identification documents, etc.
  - Verifying the attributes of the person responsible for a customer's transactions when they visit the bank teller to open an account (verification as to whether the person is part of the anti-social forces, etc.)

- Checking transaction history, etc. for persons who are found to be the holders of frozen accounts as a result of periodic checking of the attributes of existing customers

The competent authorities have made improvements and corrections with respect to these matters by providing instructions, etc. to deposit-taking institutions.

(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/CTF measures. In addition, the JBA continually exchanges information with foreign banking associations and the like as it develops organizational measures against domestic and international ML/TF. In April 2018, the "Public-Private Partnership Conference for AML/CFT" was established to facilitate cooperation between the government and private sector and to further improve countermeasures against money laundering. Efforts are also underway by the Conference to build common recognition of countermeasures against money laundering between the government and private sector and throughout in the finance industry as a whole. This has led to establishing an AML/CFT Measure Support Division within the Association to exchange views and share information about common issues in the banking industry, translate important overseas documents, etc. to further increase the capabilities of the banking industry's AML/CFT system.

The National Association of Shinkin Banks has also introduced support for AML/CFT measures among Shinkin banks by establishing a study group for AML/CFT countermeasure management systems. The group studies cases with external experts in collaboration with the Financial Services Agency, the National Police Agency, etc. regarding information, and returns the results to the Shinkin banks. In addition, the Community Bank Shinyo Kumiai has organized a joint working group with the Federation of Credit Cooperative to raise the standard of AML/CFT measures among credit cooperatives in the country.

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.

The following are recognized as examples of actions by deposit-taking institutions to implement the risk-based approach:

- For those related to risk identification
  - Specific risks are specified by considering not only the descriptions in the NRA-FUR, but the purposes of the descriptions. For example, foreigners staying in Japan as a student or technical intern on the condition that they go back to their home countries may illegally sell their accounts when they go back to their home countries, and there is a possibility that illegal funds are mixed with transactions by business operators that handle significant cash.
  - A transaction related to a business that handles products possibly used for military purposes is specified explicitly as a high-risk transaction in light of the information published by competent authorities.
  - STRs are analyzed and an independent risk index is created by looking at the trends for countries and areas of destination and origin with respect to overseas remittances, trends for nationalities with respect to accounts under the names of foreigners, and trends for occupation or business type with respect to customers.
  - Transactions using ordinary deposit accounts under foreigners' names, in which transactions such as salary transfers stopped, or corporate accounts that were opened by applying at the bank counter but their actual activities could not be sufficiently ascertained during on-site visits, are specifically identified as high-risk transactions.
- For those related to risk assessment
  - Since the sales performance regarding products, customer attributes, geographical characteristics, etc. vary from one branch office to another, each branch office conducts its own independent analysis focusing on products and services, transaction type, country/region, and customer attributes.

- A customer reported in an STR in the past is evaluated as a high-risk customer according to the content of the report.
- Domestic exchange transactions are categorized into general transfers, salary transfers, tax payments, public utility charges, outward remittances, incoming remittances, and so on, and the risks of each category are assessed.
- For correspondent management, risk is evaluated by focusing on the correspondent's business area, attributes, business content, and the presence or absence of penalties related to ML/TF.

○ For those related to the risk-based approach

- To deal with customers who were reported in STRs in the past, a system that enables information-sharing was established, and transaction details are confirmed by checking the documents and interviewing them, and the transaction is approved by a senior manager.
- Customer categories to be aware of when opening accounts are set (by classifying them as those who live in remote areas, those who open multiple accounts, those who open an account with a small deposit, those who present a residence card whose period of stay is about to expire, etc.). If a customer falls under one of the above categories, additional questions will be asked to confirm the rationality of opening the account. Additionally, if it is difficult to judge the rationality, the decision to open an account is made after checking with a senior manager.
- Banks have an internal rule whereby accounts of persons who live in a remote area, or accounts of corporations that have just relocated or been established, etc., are designated as accounts to be monitored. If any request for a transfer to such accounts is received, a check is performed to ensure the request is consistent with the purpose of opening the account, along with the intent of the person requesting the transfer; and if the consistency cannot be confirmed, the transaction is denied or reported as suspicious.
- Misuse of bank accounts is prevented by stopping accounts without any deposit and withdrawal transactions for a long time and checking the identification documents, passbooks, etc. of customers who wish to resume transactions.
- By checking the visa length of customers who are foreign students or workers, the risk of their accounts being sold when they return home is managed on a system.
- Rating is reviewed after checking the prospects for renewal of the status of residence and communicating with each customer to confirm their evidences such as residence certificate.
- The headquarters, etc. of corporate customers that start new foreign exchange transactions are visited by a person from the headquarters or branch office before transactions are started, a record of visits is created by conducting an interview about business and transaction details, etc., and the consistency between the content of any request for remittance and the visit record is verified each time a request is made.
- The case-by-case approval process is clarified whereby, for example, a checklist for foreign remittances is prepared so bank tellers of branch offices can perform checks based on the list, and a general manager is required to verify and report to the responsible division at the headquarters.
- A business operator's environment, strategy, geographical characteristics in the sales area, and customers' characteristics are analyzed to extract unique risk indicators from the geographical characteristics of their business areas, such as being close to airports and ports. The business operator identifies vendors that may dismantle, purchase, or export stolen vehicles. On top of that, the business operator assumes a high risk of money laundering in overseas remittances for the relevant company. The business operator then formulates a checklist for overseas remittance of the vendors for strict verification.
- Overseas remittances using cash brought in are suspended.
- Transaction monitoring is conducted in non-face-to-face transactions, which focuses on access information, such as IP addresses and browser languages, while considering the possibility of fake identities being used.

D. 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 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 unnatural manner and frequency in light of the purpose of the account holders' transactions, occupations, business contents, etc.

---

*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.

- Transactions involving deposits and withdrawals using the accounts of customers who have multiple accounts (including accounts held under different names using store names, etc.)

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

A. Risk Factors

(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:

- ○ Non-life insurance money derived from fraud was transferred to an account in the name of another person.

B. Trends of STRs

The number of STRs submitted by insurance companies, etc. between 2018 to 2020 was 8,182 (6,993 reports for life insurance, 1,131 reports for general insurance, and 58 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 (5,716 reports, 81.7%)
- ○ Damage insurance
  - • Transactions related to Boryokudan gangsters or their related parties (525 reports, 46.4%)

---

*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 cooperatives) of the Act on Prevention of Transfer of Criminal Proceeds.

- Unnatural transactions or transactions related to customers who show unnatural behavior or movements based on the knowledge and experience of staff (67 reports, 5.9%)

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires insurance companies etc. to conduct verification at the time of transactions, and prepare and preserve verification records and transaction records when they make contracts of insurance with cash accumulation features, when a contractor of such insurance is changed, when they pay mature insurance claims, cash surrender value, etc. of such insurance, or pay cash of more than 2 million yen.

Moreover, in addition to the supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, the Insurance Business Act stipulates that competent authorities can ask insurance companies to submit reports, conduct on-site inspections of insurance companies, and order insurance companies to make business improvements if necessary.

In the Comprehensive Guidelines for Supervision of Insurance Companies, focal points include the development of internal control systems for conducting verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds.

(b) Measures by competent authorities

The Financial Services Agency requires insurance companies, etc. to establish and maintain a risk control system against ML/TF based on the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism. In addition, the Financial Services Agency keeps track of the current status of compliance with laws and regulations and risk control by checking documents and issuing report submission orders, uses gap analysis, etc. to perform risk assessments on the types of businesses or insurance companies based on the Guidelines mentioned above. The Agency also provides guidance, supervision, etc. corresponding to the risks of each insurance company, etc. based on the assessment results.

Furthermore, in cooperation with other ministries and industry associations, the Financial Services Agency continuously provides lectures and trainings to financial institutions to improve AML/CFT measures. In 2020, 77 lectures and trainings were given. They strive to improve system development at financial institutions nationwide by explaining the purpose of the guideline revision and the main points for conducting continuous CDD.

The following matters are those that insurance companies, etc. should note in light of the actual status identified by the competent authorities:

- Establishing a system for verification at the time of transaction according to the risk and ongoing CDD
- Comprehensively and concretely identifying and evaluating risks by not only quoting the content of NRA-FURs and widely used templates, but also taking into account the characteristics of each company’s transactions, etc., including products, services, transaction types, the countries/regions involved in transactions, and customer attributes when preparing or reviewing the documents prepared by specified business operators
- Considering the introduction of an IT system or making setting changes for the existing system depending on the risks they face according to their business scales, characteristics, and transaction types
- Establishing and developing an appropriate system for transaction filtering to detect transactions subject to sanctions according to risks
- Complying with domestic and foreign laws and regulations under which sanctions may be enacted, taking other necessary measures, and building a framework to detect high-risk customers accurately

The competent authorities have made improvements and corrections with respect to these matters by providing instructions, etc. to insurance companies, etc.

(c) Measures by industry associations and business operator

In order to prevent insurance from being misused for wrongful fundraising, the Life Insurance Association of Japan and General Insurance Association of Japan 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.

The following are examples of efforts by insurance companies, etc. to implement the risk-based approach:

- The inherent risk associated with cash transactions is regarded as high risk, so the receipt of cash for insurance premiums, repayment of loans to policyholders, etc. is canceled.
- Generally, cashless insurance payment is also promoted by making payments to the accounts of the principals for which money is held. When a cash transaction is made for unavoidable reasons and the cash transaction exceeds a certain amount, a questionnaire, etc. using specified check sheets, etc. is conducted and the approval of a supervisor is required.
- Transaction conditions, etc. are recorded by the system in order to manage them after transactions have been completed.

D. 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 suspected 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]

A. Risk Factors

(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 2021, there were 4,784 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 38.

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 682.3292 trillion yen in 2020 (see Table 25).

For commodity derivative transactions, the trading volumes were about 15.16 million sheets[*2] at the Tokyo Commodity Exchange and about 0.46 million sheets in 2020 at the Osaka 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 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 25 [Transaction Volume of Stocks]

Year / Category	2018	2019	2020
First Section, TSE	740,746,041	598,213,662	671,671,658
Second Section, TSE	11,006,506	6,188,491	10,657,529
Total	751,752,547	604,402,153	682,329,187

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 (Specially permitted investment management business for Offshore Professional 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.
- Criminal proceeds derived from embezzlement were invested in commodity derivatives.

B. Trends of STRs

The numbers of STRs submitted by financial instruments business operators, etc. and commodity derivatives business operators between 2018 and 2020 were 48,394 and 626, 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 (13,126 reports, 27.1%)
- Commodity derivatives business operators
  - Transactions in which it was suspected that the customer was using a fictitious or other person's name (379 reports, 60.5%)

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires financial instruments business operators, etc. and commodity derivatives business operators that handle investment instruments to conduct verifications at the time of transactions, and prepare and preserve verification records and transaction records when opening accounts or dealing with products and services.

Furthermore, in addition to the supervisory measures under the Act on Prevention of Transfer of Criminal Proceeds, the Financial Instruments and Exchange Act and the Commodity Derivatives Act stipulate that competent authorities may ask business operators to submit reports, conduct on-site inspections of business operators, and order business operators to make business improvements if necessary.

In addition, the Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc. and Commodity Derivatives Business Operators include focal points on the development of an internal control system for conducting verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds.

(b) Measures by competent authorities

The Financial Services Agency requires financial instruments business operators, etc. under its jurisdiction to establish and maintain a risk control system against ML/TF based on the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism. The Financial Services Agency also keeps track of the current state of compliance with laws and regulations and risk control by checking documents and issuing report submission orders, uses gap analysis, etc. to perform risk assessments on the types of businesses or operators based on the Guidelines mentioned above. The Financial Services Agency also provides guidance, supervision, etc. corresponding to the risks of operators based on the assessment results. As part of its year-round monitoring activities for financial instruments business operators, etc., the Financial Services Agency verifies the current statuses of measures taken for AML/CTF. Furthermore, in cooperation with other ministries and industry associations, the Financial Services Agency continuously provides lectures and

trainings to financial institutions to improve AML/CFT measures. In 2020, 77 lectures and trainings were given. It is working to improve system development at financial institutions nationwide by explaining the purpose of the guideline revision and the main points for conducting ongoing CDD. The Securities and Exchange Surveillance Commission annually publishes the *Overview of Securities Businesses Monitoring and Case Studies*, which introduces examples of inadequate internal control systems related to AML/CFT.

The Ministry of Agriculture, Forestry and Fisheries, and Ministry of Economy, Trade and Industry require commodity derivatives business operators under their jurisdiction to establish and maintain a risk management system in accordance with the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Commodity Derivatives Business (published on August 14, 2019 by the Ministry of Agriculture, Forestry and Fisheries, and Ministry of Economy, Trade and Industry, and revised on October 19, 2021). They also check the actual situation with regard to legal compliance and risk management through a written survey. The Ministries also conduct risk assessment for each commodity derivatives business operator through a gap analysis, etc. based on the Guidelines, and provide guidance and supervision, etc. corresponding to the risk of the respective commodity derivatives business operators based on the assessment results, etc. Furthermore, as a part of their monitoring activities for commodity derivatives business operators, the Ministry of Agriculture, Forestry and Fisheries, and Ministry of Economy, Trade and Industry verify the current status of measures taken for AML/CTF.

The Ministry of Land, Infrastructure, Transport and Tourism, etc. also issues report submission orders to grasp the actual status of compliance with laws and regulations and risk control by specified joint real estate enterprises, etc.[*1] and it provides guidance and supervision corresponding to the risks of respective specified joint real estate enterprises based on the information obtained through the issued orders.

The following matters are the main points that business operators should note in light of the actual situation identified by the competent authorities:

- When preparing the documents to be prepared by specified business operators, etc. conduct an appropriate risk assessment and record the basis for the risk assessment and judgment history so that they can be checked later, and describe businesses and risk mitigation measures corresponding to the actual situation in the documents.
- Establish a system for severing relationships with anti-social forces, for example by periodically checking, even after opening an account, if a customer falls under the definition of anti-social forces, and refusing transactions with customers who are strongly suspected to be Boryokudan members.
- The supervisor under the Act on Prevention of Transfer of Criminal Proceeds should make decisions as to whether to stop or resume a transaction with a customer who is suspected to have committed impersonation. When resuming a transaction, take appropriate measures such as requesting the customer to submit supplementary documents such as customer principle identification documents and others that are different from those submitted at the time of opening the account, along other supplementary documents.
- Appropriately investigate the presence or absence of impersonation by periodically performing name-based aggregation and extracting customers with different names who share the same e-mail addresses, etc. If customers with different names who share the same e-mail addresses, etc. have been extracted, instead of just requesting customers to update their e-mail addresses, etc., conduct an investigation to determine whether impersonation has occurred.
- For customers who have declared that they are foreign PEPs, take appropriate measures, such as enhanced CDD, after checking the relevant details corresponding to risks.
- Take appropriate measures to confirm the beneficial owners of corporate customers, by utilizing not only the customers' declaration but information from third-party organizations.
- For foreign customers, take appropriate measures such as confirming the period of stay, preserving the evidence, and requesting additional materials when the stay expires.
- Advance the level of transaction monitoring sophistication, such as adding monitoring scenarios for deposit and withdrawal and grasping transactions from overseas by detecting IP addresses.
- In case of transactions involving a transfer of the value of property, such as remittances from or to a person whose name is different from the account name, or a transfer of securities, etc. between

*1 Meaning the persons listed in Article 2, paragraph 2, item 27 of the Act on Prevention of Transfer of Criminal Proceeds.

accounts under different names, take appropriate measures, such as checking the reasons for the transactions and checking for the presence or absence of any suspicious transactions.

- For high-value over-the-counter cash transactions, confirm and record the reasons for using such transactions and the payment route (whether or not the payment is made with the customers' funds), and verify the existence of suspicious transactions.
- Monitor cash deposits and withdrawals using ATMs. If an unnatural transaction is found, e.g., a large amount of deposit or withdrawal is made through frequent repetition of ATM deposits or withdrawals in a short period, check the split deposits or withdrawals are reasonable. Then respond appropriately, such as filing STRs if necessary.
- Identify groups that engage in illegal transactions based on terminal identifiers or take other appropriate measures to prevent market manipulation by groups who are colluding and conspiring with each other.
- Establish and develop an appropriate system for transaction filtering to detect transactions subject to sanctions according to risks.
- If there is a suspicious transaction of wash sales, etc. based on inquiries from overseas regulatory authorities, take appropriate measures such as filing STRs.
- When a problem may be recognized through the indications of competent authorities or self-regulatory organizations, appropriate improvement measures should be established, and the progress of them should be verified through internal meetings and internal audits so that sufficient improvements can be made.
- Within the group, share necessary information and build a reporting system to strengthen cooperation.

The competent authorities are making improvements and corrections with respect to these matters by providing instructions, etc. to financial instruments business operators and commodity derivatives business operators, etc.

(c) Measures by industry associations and business operator

The Japan Securities Dealers Association[*1], the Commodity Futures Association of Japan[*2], and the Type II Financial Instruments Firms Association created Q&As or other materials regarding the Act on Prevention of Transfer of Criminal Proceeds, etc. and held training seminars in 2020 to support AML/CFT measures taken by members.

The Japan Securities Dealers Association partially revised the Member's Concept of Notification of Suspicious Transactions to continuously deepen the understanding of members and strive to make appropriate notifications. In addition, the Association shows specific examples and matters to note that are useful for members with respect to the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism prepared by the Financial Services Agency through activities such as trainings and audits.

The Commodity Futures Association of Japan also shows specific examples and matters to note that are useful for member companies when dealing with actual business relating to the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism for the Commodity Derivatives Business prepared by the Ministry of Agriculture, Forestry and Fisheries and the Ministry of Economy, Trade and Industry, and promotes appropriate responses to ML/TF. As for the system to inquire if a customer is part of the anti-social forces established in April 2019, according to the "Regulations on the Exclusion of Anti-social Forces" and the "Terms of Use of Anti-social Force Inquiry System," the Commodity Futures Association of Japan receives inquiries from members about customers of commodity derivatives transactions. In July 2020, due to the transfer of listed commodities, the terms of use for the system were partially amended to accept

---

*1 The Japan Securities Dealers Association is a self-regulatory organization that has been approved under the Financial Instruments and Exchange Act. The Association makes efforts to soundly develop the industry and protect investors, with measures that include setting up self-regulatory rules. As of the end of March 2021, 268 Type I financial instrument business operators are members of the Association, and they are obliged to comply with the Association's rules.

*2 The Commodity Futures Association of Japan is a self-regulating organization that is approved under the Commodity Derivatives Act. The Association conducts various self-regulation works regarding commodity derivatives business to foster fair and smooth commodity derivative transactions and protection of clients. All commodity derivatives business operators have joined the Association, and they are obliged to comply with the Association's rules.

inquiries from members who are involved in commodity-related market transactions under the Financial Instruments and Exchange Act.

As part of their efforts to apply a risk-based approach in accordance with the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism prepared by the Financial Services Agency, the Investment Trusts Association, Japan has created a practical manual for members on implementing AML/CFT measures at investment trust management companies that investment trust companies and investment companies contract for asset management. From the viewpoint of the efficient implementation of the measures, the Association supports the promotion of the efforts by continuously holding an expert committee meeting in the Association. The Association also promotes the efforts to unify the questionnaire format so that asset management companies can verify the AML/CFT measures of sales companies efficiently.

The Japan Investment Advisers Association conducts surveys that include questions about the actions made by its members for AML/CFT measures, shares the survey results with its members, and raises the members' awareness for performing voluntary comprehensive inspections.

The Association for Real Estate Securitization provides support to its members for taking AML/CFT measures by explaining the overview of the Act on Prevention of Transfer of Criminal Proceeds and matters to be noted relating to the information verified at the time of transactions, etc. during the compliance training provided for the members twice each year.

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, screen out transactions that are likely to pose ML/TF risks, and rigorously conduct CDD.

Furthermore, with respect to products and services, etc. provided through financial instruments business operators, etc., it is stipulated in the general conditions for financial instruments business operators or other documents that, in principle, funds can only be transferred to accounts with the customers' names, but not to third parties. If remittances and payments by different names are properly controlled, this can be considered as a measure to mitigate the risk of misuse for money laundering to some extent.

The following are examples of efforts by financial instruments business operators and commodity derivatives business operators to implement the risk-based approach:

- Confirmation and management of foreign customers' periods of stay, confirmation of the beneficial owners of legal persons using a third-party information agency, and freezing and suspending the transactions of non-operating accounts as an example of enhanced CDD.
- Transaction monitoring is promoted by adding deposit and withdrawal monitoring scenarios and keeping track of overseas transactions by detecting IP addresses.
- In light of risks associated with cash transactions, cash transactions are prohibited.
- Necessary information is shared and the reporting system is strengthened as an initiative among companies in the same financial group.

D. 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 joint real estate enterprises as specified business operators. It is recognized that there is a risk of misuse for the transfer of criminal proceeds in the joint real estate business, which comes from distributing profits arising from the execution of a joint real estate business contract (including a contract for promising the distribution of proceeds from real estate transactions made by delegating the performance of services to one or some of the parties providing funds as a joint business financed by the funds) and which can be used as a way to make it difficult to trace criminal proceeds.

*2 Article 2, paragraph 2, items 34 and 35 of the Act on Prevention of Transfer of Criminal Proceeds lists book-entry transfer institutions and account management institutions as specified business operators. It is recognized that the products and services handled by book-entry institutions, which perform services related to book-entry that generate the effect of transferring or pledging bonds and stocks, etc., and account management institutions, which open accounts for the book-entry transfer of bonds, etc. for others (which can be performed by securities companies, banks, etc.), may be misused for the transfer of criminal proceeds.

(4) Trust Dealt with by Trust Companies etc.[*1]

A. Risk Factors

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 by a Financial Institution (Act No. 43 of 1943). As of the end of March 2021, 86 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 abovementioned characteristics.

B. Trends of STRs

There were 50 STRs[*2] related to trusts from 2018 to 2020. 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 (25 reports, 50.0%)
- Unnatural transactions or transactions related to customers who show unnatural behavior or movements based on the knowledge and experience of staff (7 cases, 14.0%)

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires a specified business operator who is/will be a trustee to conduct verifications at the time of transactions against not only settlors but also trust beneficiaries when executing the conclusion of a trust contract or the conclusion of a judicial relationship with a trust beneficiary through acts, including acts of trust, acts of designating a beneficiary, and acts of transferring the right to be a beneficiary; provided, however, that this does not apply to all trusts.

Moreover, in addition to the supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, the Trust Business Act and the Act on Engagement in Trust Business by a Financial Institution

---

*1 Refers to the person listed in Article 1, 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.

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

As well, the Comprehensive Guidelines for Supervision by the Financial Services Agency indicate focal points for trust companies and financial institutions that operate trust business with respect to the development of internal control systems for verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds. Trust companies 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 regulations and manuals, provide periodic trainings, conduct internal audits, screen out transactions that are considered to be of high risk, and adopting enhanced monitoring of high-risk transactions.

Moreover, trustees are required to submit records that include beneficiaries' names to tax authorities under the tax law, with the exception of some trusts. This is not for directly preventing ML/TF, but to help competent authorities identify trust beneficiaries within a certain scope.

In addition, funds related to trusts, such as proceeds from trust assets and payment for a trust beneficiary right, are transferred through deposit and savings accounts. Therefore, it can be said that there is a double layer of measures to mitigate risks for such transactions of assets, which include legal regulations against ML/TF in the deposit-taking institution sector, supervision by competent authorities, and voluntary actions by the industry and business operators.

(b) Measures by competent authorities

The Financial Services Agency requires trust companies, etc. to establish and maintain a risk control system against ML/TF based on the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism.

The Financial Services Agency also keeps track of the current state of compliance with laws and regulations and risk control by checking documents and issuing report submission orders, uses gap analysis, etc. to perform risk assessments on the industry, trust companies, etc. based on the Guidelines mentioned above. The Financial Services Agency provides guidance, supervision, etc. corresponding to the risks of trust companies, etc. based on the assessment results.

Furthermore, the Financial Services Agency continuously provides lectures and trainings for other ministries, industry associations and financial institutions to improve AML/CFT measures. In 2020, 77 lectures and trainings were given. It is working to improve system development at financial institutions nationwide by explaining the purpose of the guideline revision and the main points for conducting ongoing CDD.

The following are the main points to which trust companies, etc. should pay attention in light of the actual situation identified by the competent authorities:

- When analyzing risks, do so comprehensively and concretely, including analyzing STRs and reflecting them in documents to be prepared by specified business operators.
- Confirm verification at the time of transaction according to the risk. Besides, conduct customers' risk assessment based on products, services, transaction types, countries, regions, customer attributes, and build a system of ongoing CDD.
- Establish and develop a system for transaction filtering appropriately to detect transactions subject to sanctions according to risks.
- It is necessary to hire staff with expertise and suitability for the sales department, management department, and audit department, and to provide training for such staff.

The competent authorities have made improvements and corrections with respect to these matters by providing instructions, etc. to trust companies, etc.

(c) Measures by industry associations and business operator

The Trust Companies Association of Japan supports 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.

The followings are recognized as examples of efforts by trust companies, etc. to implement the risk-based approach:

- Risk assessment is performed for each customer while considering the products, services, transaction types, countries, regions, and customer attributes, and measures are taken according to the assessment.
- CDD is implemented according to the settlors and trustees' risks, while considering that the actual right holders and their assets may be obscured due to the trust relationship, and verifications are continuously conducted to determine whether or not business partners are anti-social forces or persons subject to economic sanctions.

D. 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]

A. Risk Factors

(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 (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 2021, there were 1,638 registered business operators, while the outstanding balance of loans was 32.9625 trillion yen at the end of March 2021.

(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, and the loan was transferred to the same account.

B. Trends of STRs

The number of STRs submitted by money lenders, etc. was 54,967 between 2018 and 2020.

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.

- Deposits or withdrawals using accounts suspected to be opened by a fictitious or borrowed name (21,154 reports, 38.5%)
- Unusual transactions or transactions related to customers who show unusual behavior or movements, based on the knowledge and experience of staff (11,595 reports, 21.1%)

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires to conduct verification at the time of transactions, and to prepare and preserve verification records and transaction records on money lenders etc. when they make a contract to lend money.

In addition to the supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, the 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. Comprehensive Guidelines for Supervision of Money Lenders set out points to consider when

---

*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.

establishing internal control systems for conducting verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds.

(b) Measures by competent authorities

The Financial Services Agency requires money lenders to establish and maintain a risk control system against ML/TF based on the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism.

The Financial Services Agency also keeps track of the current state of compliance with laws and regulations and risk control by checking documents and issuing report submission orders, and uses gap analysis, etc. to perform risk assessments on the industry, money lenders, etc. based on the Guidelines mentioned above. The Financial Services Agency provides guidance, supervision, etc. corresponding to the risks of money lenders, etc. based on the assessment results.

Furthermore, the Financial Services Agency continuously provides lectures and trainings for other ministries, industry associations and financial institutions to improve AML/CFT measures. In 2020, 77 lectures and trainings were given. It is working to improve system development at financial institutions nationwide by explaining the purpose of the Guidelines revision and the main points for conducting continuous CDD.

The following matters are the key points to which money lenders, etc. should pay attention in light of the actual situation identified by the competent authorities:

- When creating and reviewing documents to be prepared by specified business operators, they should quote the contents of the NRA-FUR and widely used templates. They should also consider the characteristics of their companies' transactions such as products, services, transaction types, countries and regions related to transactions, customer attributes, etc., and comprehensively and concretely identify and assess risks.
- It is necessary to establish a system of verification at the time of transactions and ongoing CDD according to risks.
- It is necessary to consider introducing IT systems and changing the settings for existing systems, based on the risks faced according to the scale and characteristics of one's own business and transaction types.
- It is necessary to build a framework to detect high-risk customers accurately.

The competent authorities are trying to improve and correct these matters by giving guidance to money lenders, etc.

(c) Measures by industry associations and business operator

The Japan Financial Services Association has 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.

Examples of actions by money lenders, etc. to implement the risk-based approach are as follows:

- Phone numbers provided by customers are checked against a business operator's database to ascertain that the numbers are real.
- Suspicious and unnatural transactions are detected by utilizing IT vendors' systems and checking when the telephone numbers provided by the customers were installed.

D. 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

A. Risk Factors

(a) Characteristics

A funds transfer service means an exchange transaction service (it is necessary to register the type corresponding to the amount of each remittance[*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 2021, there were 80 registered business operators. There were 480.69 million remittances totaling 2.3484 trillion yen in fiscal 2019. 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 26).

There are three main remittance methods in funds transfer services as follows:

(1) A client requests a funds transfer by bringing cash to the sales office of a funds transfer service provider and the recipient receives cash at another sales office of the provider;

(2) Funds are transferred between a client's account and a recipient's account opened at a funds transfer service provider or between customers' accounts opened on the website, etc. of the funds transfer service provider; and

(3) A funds transfer service provider issues a card or an instrument (money order) corresponding to money recorded in its server, and payment is made to the person who owns the card or a person who brought in the instrument.

Funds transfer services may involve a client giving face-to-face instructions to a funds transfer service provider to remit money, or also give non-face-to-face instructions to remit money by using mail, the Internet, etc. Recipients can receive payment, etc., in various ways, such as receiving cash or a money order and depositing it into a bank account. Various business models are being developed, and risks exist in different areas for each funds transfer service provider, depending on the various services that each provider is developing. For example, 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 amount, business scale, and characteristics appropriately. The Financial Services Agency mentioned that many funds transfer service providers do not comprehensively or concretely identify and assess their risks and they carry out perfunctory verifications at the time of transactions with no customer risk assessment or CDD. The Agency also mentioned that funds transfer service providers do not have a system suitable for expanded and diversified customer segments. 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.

---

*1 If it necessary to register for Type 1 Fund Transfer Services in the event of remittance of more than one million yen, Type 2 Fund Transfer Services in the event of remittance of one million yen or less and Type 3 Fund Transfer Services in the event of remittance of fifty thousand yen or less.

Table 26 [Trends in Funds Transfer Service Business]

Category \ Year	2017	2018	2019
Number of remittances per year	84,071,614	126,199,274	480,687,760
Transaction volume per year (million yen)	1,087,737	1,346,370	2,348,439
Number of registered funds transfer service providers	58	64	75

Note: Data from the Financial Services Agency

(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 remit money overseas 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 cash derived from selling cars obtained through fraud to a foreign country 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.
- An illegal foreigner 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 a funds transfer services.

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.

B. Trends of STRs

The number of STRs submitted by funds transfer service providers was 11,344 between 2018 and 2020.

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.

- Transactions having unnatural characteristics or conducted at an unnatural frequency considering the purpose of the transactions, occupation or business of the client, etc. (2,000 reports, 17.6%)
- Transactions related to Boryokudan gangsters or their related parties (1,436 reports, 12.7%)

---

*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.

- 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 (1,129 cases, 10.0%)
- 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 (1,082 cases, 9.5%)

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.

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires Funds Transfer Services Providers to conduct verification at the time of transactions, and prepare and preserve verification records and transaction records when they conduct foreign exchange transactions etc. that involve the payment and receipt of cash exceeding 100,000 yen.

In addition to the supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, the Payment Services Act provides that the competent authorities can require submission of reports from, conduct on-site inspection of and issue business improvement orders etc. to funds transfer service providers if necessary. The Payment Services Act also provides grounds for refusing or rescinding the registration of a funds transfer service provider, including a corporation that has not established a system that is necessary for the proper and secure provision/conducting of funds transfer services.

Furthermore, the Guidelines for Administrative Processes by the Financial Services Agency set out points to consider when establishing internal control systems for conducting verifications at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds. When business operators apply to register as a funds transfer service provider, these points are also included in the items to check related to the requirements for establishing a system to provide funds transfer services properly and securely.

As described above, a system for the competent authorities to provide AML/CFT guidance and supervision has been established.

(b) Measures by competent authorities

The Financial Services Agency requires that funds transfer service providers establish and maintain a risk control system against ML/TF based on the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism and grasp the current state of compliance with laws and regulations and of risk control.

In addition, the Financial Services Agency keeps track of the current state of compliance with laws and regulations and risk control by checking documents and issuing report submission orders, uses gap analysis, etc. to perform risk assessments on the industry or funds transfer service providers. The Financial Services Agency also provides guidance, supervision, etc. corresponding to the risks of each funds transfer service provider based on the assessment results.

Furthermore, the Agency is strengthening its efforts on supervision where transfer transactions are particularly emphasized by conducting research on transfer transactions.

In addition, the Financial Services Agency continuously provides lectures and trainings for other ministries, industry associations and financial institutions to improve AML/CFT measures. In fiscal 2020, 77 lectures and trainings were given. It is working to raise the level of system development at financial institutions nationwide by explaining the purpose of the guideline revision and the points of view for ongoing CDD.

In light of the actual situation identified by the competent authorities, the key points to which funds transfer service provider s should pay attention are as follows:

- A funds transfer service provider that has diverse business models, etc. should not only identify and assess the risks of individual products and services but also conduct company-wide identification and assessment of risks comprehensively and concretely.

- Funds transfer service providers should conduct an overall risk assessment of services provided in collaboration with the services of other business operators, such as account transfer services provided by banks, and should clarify the division of roles and responsibilities with collaborators. They should also check the information on users and take appropriate and effective measures to prevent misconduct by cooperating with collaborators.
- Allocating sufficient personnel in departments in charge of AML/CFT measures and thereby securing personnel with the necessary expertise and ability.
- A system for verification at the time of transaction and ongoing CDD must be established according to the risk.
- Establish a system to appropriately examine and manage agents and implement monitoring and training regularly or as necessary.
- If there are customers who open an account by conducting verification at the time of transaction through a procedure of bank account transfer, conduct a pre-screening on their relationship with antisocial forces, in addition to confirming that they are not impersonating, at the time of opening their account.
- The accuracy of the verification of customer information, including identification data (name, address, and date of birth), purpose of transactions, and occupation, at the time of transactions must be ensured before implementing AML/CFT measures.
- When persons subject to economic sanctions are designated by a resolution of the United Nations Security Council, such persons should be added to the provider's list of persons subject to sanctions within several hours or 24 hours at the latest, and transaction filtering should be conducted to immediately check if there is any difference with existing customers.

The competent authorities have made improvements and corrections with respect to these matters by providing instructions, etc. to funds transfer service providers.

(c) Measures by industry associations and business operator

The Japan Payment Service Association, industry association, supports 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. In addition, the association has published the Guidelines for Preventing Misconduct in Collaboration with Bank Accounts due to the occurrence of illegal withdrawals from a bank account through the payment services of a funds transfer service provider in September 2020. The association describes the concept and examples of measures that funds transfer service providers should take to prevent misconduct. For example, the association requires funds transfer service providers to perform risk assessments of the account transfer services of collaborating banks and implement measures to prevent misconduct in cooperation with collaborators.

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.

Business categories of funds transfer service providers vary. Some of them, for example, those that conduct international remittances to many countries or handle customers without conducting the proper checks, are at risk of being misused for ML/TF. On the other hand, some providers that deal with only refunds for the return of goods or cancelled contracts provide limited services. Furthermore, although the scale of funds transfer service providers varies from large companies listed in the First Section of the Tokyo Stock Exchange to small and mid-sized enterprises, as the nature of business to be handled is the same, the specific risks of misuse for ML/TF do not differ much among them. However, although it is acknowledged that large-scale fund transfer services providers have established sufficient internal control systems to date, small and medium-sized enterprises are still lagging behind. In response, the Financial Services Agency is working to improve the countermeasures against ML/TF in the industry as a whole by providing appropriate guidance and supervision, including administrative guidance for funds transfer service providers whose efforts are insufficient.

The following are examples of efforts by funds transfer service providers to implement the risk-based approach:

- Risk is evaluated for each customer by taking into account the customer attributes and transaction conditions, and measures are taken according to the assessment.
- When a funds transfer service provider engages in the issuance of pre-paid cards as a side business, risks are also identified and evaluated for the services it provides as an issuer of pre-paid cards.
- Cases where upper limits are set for transaction amounts according to the product/service, transaction type, country/region, or customer attributes, and transactions exceeding those amounts are severely scrutinized (for example, upper limits for transaction amounts vary depending on visa status, such as permanent resident, technical intern, student studying abroad, etc.)
- Cases where a resident card is presented as the principle identification document to confirm the period of stay and its period is controlled by using system when conducting a transaction with a foreigner

D. Assessment of Risks

Funds transfer services can be a useful method for ML/TF, given the characteristics of funds transfer services in which foreign exchange transactions are performed as a business, as well as the existence of funds transfer service providers that offer services to remit to many countries and the existence of type I funds transfer services, which allow large amounts of foreign exchange transactions.

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, the fact that their use is expected to increase due to the increasing number of foreign residents in Japan, 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 unnatural characteristics or conducted at an unnatural 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

A. Risk Factors

(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 2021, 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.

These cases are believed to have occurred due to circumstances in which appropriate internal control systems for various risks, including cyber security, could not keep up with the rapid expansion of the business scale of operators that started providing crypto-assets exchange services.

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.[*1] 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 overseas in which drug traffickers convert criminal proceeds derived from drug trafficking into bitcoins via crypto ATMs using forged identification documents, it is necessary to watch how such ATMs are actually being used overseas even though there is no crypto ATM in Japan.

(b) Typologies

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

- An offender purchased crypto-assets using illicitly acquired accounts or credit card information under another person's name, exchanged crypto-assets into Japanese yen using exchange sites in foreign countries, and transferred the proceeds to accounts under another person's name.
- An offender withdrew cash from a bank account to which criminal proceeds from specialized fraud were transferred, remitted the money to the account of a crypto-assets exchange service provider opened at an Internet bank to purchase crypto-assets, and then transferred it to multiple accounts.
- An offender transferred crypto-assets obtained through computer fraud to an account at an overseas crypto-assets exchange where an account can be opened with 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

---

*1 The names of crypto-assets handled by crypto-assets exchange service providers used to be notified after the preliminary examination at the Japan Virtual and Crypto Assets Exchange Association which is a certified industry association (actually through consultation with the Financial Services Agency in advance) so that the administration can handle these crypto-assets appropriately. The amended Payment Services Act requires prior notification.

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.

The following cases are common examples of violating the Act on Prevention of Transfer of Criminal Proceeds in which an offender impersonates another person and accepts the required user account ID and passwords for the purpose of receiving services under a contract for crypto-assets exchange with a crypto-assets exchange service provider:

- A case in which the ID and password of a crypto-asset account opened by a Vietnamese resident in Japan were provided to a third party on an illegally paid basis.
- 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:

- Crypto-assets were used for transactions of illegal drugs or for payment of special points that were necessary to download child pornography.
- Crypto-assets were used for ransomware payment.

B. Trends of STRs

The number of STRs submitted by crypto-assets exchange service providers between 2018 and 2020 was 21,115.

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.

- 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 (2,340 cases, 11.1%)
- Unnatural transactions or transactions related to customers who show unnatural behavior or movements based on the knowledge and experience of staff (1,429 cases, 6.8%)
- Transactions related to accounts in which crypto-assets are remitted to many addresses frequently, especially in cases where large amounts of crypto-assets are deposited immediately before withdrawal (851 cases, 4.0%)
- Unnatural patterns of transactions made with unnatural frequency in light of the purpose of transactions confirmed when opening the account, occupation, details of business, etc. (833 cases, 3.9%)

The details of transactions that are suspected to be made with fictious 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

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires crypto-assets exchange service providers to conduct verification at the time of transactions and to prepare and preserve the verification records and transaction records when concluding contracts concerning continuous or repeated exchange of crypto-assets

(conclusion of contracts to open accounts), when converting crypto-assets worth more than 100,000 yen and when transferring crypto-assets of customers, etc., worth more than 100,000 yen upon the customers' request.

Furthermore, the Act on Prevention of Transfer of Criminal Proceeds prohibits the act of impersonating another person and accepting the required ID and passwords for the purpose of receiving services under a contract for crypto-assets exchange with a crypto-assets exchange service provider.

In addition to supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, the Payment Services Act stipulate that competent authorities may ask crypto-assets exchange service providers to submit business reports, conduct on-site inspections of crypto-asset exchange service providers, and order crypto-assets exchange service providers to make business improvements if necessary. In addition, the Act also lists any corporation that has not established a system to properly and securely conduct crypto-assets exchange service business as grounds for refusing or rescinding its registration as a crypto-assets exchange service provider.

Moreover, the Guidelines for Administrative Processes by the Financial Services Agency set out points to consider when establishing internal control systems for verifications at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds. When business operators apply to register as a crypto-assets exchange service provider, these points are also included in the items to check related to the requirements for establishing a system to conduct crypto-assets exchange service businesses properly and securely.

As mentioned above, a system has been established for the competent authorities to provide guidance on AML/CFT.

In October 2018, the FATF amended the FATF Recommendations (including Recommendation 15) to require each country to introduce regulations related to AML/CFT measures as well as a license and registration system for exchange service providers of crypto-assets and legal currencies. Due to the above amendment, in June 2019, the Interpretative Notes of the FATF Recommendations and the guidance related to crypto-assets published in June 2015 were amended to include the concept regarding the risk-based approach for crypto-assets.

(b) Measures by competent authorities

To strengthen guidance and supervision on crypto-assets exchange service providers, the Financial Services Agency developed the Guidelines for Administrative Processes in April 2017 for Agency employees to oversee crypto-assets exchange service providers. In August of that year, facing increasing ML/TF risks involving crypto-assets, the FSA established the Virtual Currency (crypto-assets) Monitoring Team to strengthen guidance for and supervision of crypto-assets exchange service providers, and investigate what makes the internal systems of crypto-assets exchange service providers so effective. Based on the Guidelines, the Financial Services Agency issues warnings to corporations operating crypto-assets exchange services without the registration, and has issued 10 warnings as at the end of June 2021.

In addition, the Agency requires that crypto-assets exchange service providers establish and maintain a risk control system against ML/TF based on the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism and grasp the current state of compliance with laws and regulations and of risk control. The Agency issues report submission orders, and provides guidance or supervision, etc. corresponding to the risks to operators based on the assessment results.

The Financial Services Agency also requires crypto-assets exchange providers to develop and improve their risk assessment system and effective business operation by considering the risk-based approach accurately and to conduct verifications at the time of transactions together with customer risk assessments, or otherwise make efforts in taking measures for mitigating risks, in addition to complying with laws and regulations. For example, if crypto-assets exchange providers offer new services to improve the convenience of customers, they need to understand the risks unique to them properly as needed, and take necessary measures to mitigate risks because measures for mitigating risks used by banks and other types of businesses may not be appropriate for the risks of services provided by crypto-assets exchange services providers.

Furthermore, the Financial Services Agency continuously provides lectures and trainings for other ministries, industry associations and financial institutions to improve AML/CFT measures. In 2020, 77 lectures and trainings were given. It is working to improve system development at financial institutions nationwide by explaining the purpose of the guidelines' revision and the main points for conducting continuous CDD.

In light of the actual situation identified by the competent authorities, the key points to which crypto-assets exchange services providers should pay attention are as follows:

- As obligations under laws and regulations, if persons subject to economic sanctions, etc. are designated by a resolution of the United Nations Security Council, such persons should be added to the provider's list of persons subject to sanctions within several hours or 24 hours at the latest, and transaction filtering should be conducted to immediately check if there is any difference with existing customers.
- Each time new products or services are introduced, documents to be prepared by specified business operators, etc. should be reviewed. However, some crypto-assets exchange service providers renew such documents only once a year. It is necessary to keep such documents updated.
- Measures to mitigate risks should not be limited to the performance of obligations under laws and regulations, such as conducting verifications at the time of transactions, or to quoting the contents of the NRA-FUR and widely used templates. Regarding the results of an analysis to be compiled in a document prepared by a specified business operator, etc., describe the results of examining the sufficiency of measures to mitigate risks. Ensure that the results are reflected in the procedure of verification at the time of transaction, from the perspective of a risk-based approach that considers high-risk factors, particularly non-face-to-face transactions, and the high anonymity of crypto-assets themselves.
- It is necessary to take ongoing CDD based on the company's risk identification and assessment, including managing the period of stay of foreigners.
- When judging whether a transaction is suspicious, it is necessary not only to refer to the List of Reference Cases of Suspicious Transactions published by the Financial Services Agency, but also to make flexible decisions according to risks based on the identification and assessment of risks made by the company.
- The business section (frontline) should not only review the convenience or profitability of crypto-assets, but also assess the security risks and ML/TF risks for each crypto-assets handled to establish an internal control system corresponding to such risks.
- The risk control and compliance section (second line) should secure and train staff with the expertise and skills necessary to give advice to the frontline regarding ML/TF risks, etc. in light of the regulations for opening accounts and crypto-assets transactions, as well as the characteristics of risks of crypto-assets, etc.
- The internal audit section (third line) should secure and train audit staff with the expertise and skills necessary to implement AML/CFT measures and audit risks to systems, etc.

The competent authorities have made improvements and corrections with respect to these matters by providing instructions, etc. to crypto-assets exchange service providers,

The Financial Services Agency has imposed a total of 29 administrative dispositions, including business improvement orders, as of the end of March 2020 against crypto-assets exchange service providers, etc. There was only one administrative disposition imposed after 2019. In the industry as a whole, the system for conducting operations properly has been developed.

(c) Measures by industry associations and business operator

Crypto-assets exchange service providers themselves have also taken measures. In March 2018, 16 crypto-assets exchange service providers established a new industry association, the Japan Virtual Currency Exchange Association (which has changed its name to the Japan Virtual and Crypto Assets Exchange Association), that was certified by the Financial Services Agency in October of the same year. (In April 2020, the Association was certified as a financial instruments business association (self-regulatory organization for crypto-assets derivatives transactions).) The Association has established its self-regulatory rules and guidelines based on the Financial Services Agency's Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism, and inspects the status of compliance with laws and the self-regulatory rules by member companies, provides guidance based on inspection results, and raises member companies' awareness of offenses, etc. carried out using crypto-assets. 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.

The following are examples of efforts by crypto-assets exchange service providers to implement the risk-based approach:

- For those related to risk identification and assessment
  - A system for ensuring active involvement of the frontline sections as well as the second line sections (such as proposing primary risk assessments, participating in risk assessment meetings, etc.) has been established to conduct risk assessment for its own products and services.
  - Information or data such as the number of legal person and individual customers, percentages of customers' countries of residence and countries of origin, and types of crypto-assets and legal tender handled are taken into account in the business operators' own feature analysis.
  - A business operator comprehensively identifies and evaluates its own services, in addition to exchanging crypto-assets, etc.
  - Not only risks directly related to ML/TF, but also other risks that may have indirect impact such as hacking risk, are evaluated.
  - A business operator identifies and assesses risks for each type of crypto-assets it handles, focusing on bad reputation, liquidity, etc.
  - Increases and decreases in the use of transaction channels, etc. are verified flexibly by taking market trends into account. Services for those that are not consistent with their customer attributes are suspended, or other measures to mitigate risks are taken flexibly.
- For those related to the risk-based approach
  - An index related to suspicious transactions is extracted in light of its own past illegal remittance cases and STR analysis results and set as points to note when conducting verifications at the time of transactions, or other measures based on its own business status are improved.
  - In the crypto-assets exchange business, which is closely related to IT systems, data is effectively utilized by taking advantage of its characteristics that allow customer management to be implemented relatively easily using IT systems. For example, since the start of the business, the identification data of customers, etc. has been recorded and stored in a system, and multiple electromagnetic data sets, including transfer address data, have been utilized for monitoring using a system.
  - Risks associated with the deposit route of legal currency are identified and evaluated, and in light of such risks, measures to mitigate risks such as restricting the payment and funds-transfer frequency for a certain period for deposits made at convenience stores.
  - A business operator monitors transfer destination addresses by using a crypto-assets analysis tool in light of risks associated with the transfer of crypto-assets, and for an attribute determined as high risk, it takes risk mitigation measures such as restricting transfers.
  - As measures to mitigate the risk of services being used for specialized fraud, investigations and analyses are conducted on the trends of cases, such as when the photo, address or other registered information on a customer's identification document partially matches with another customer's registered information and impersonation is suspected. The investigation and analysis results are used to make changes to the documents to be prepared by specified business operators, etc. as necessary, and verifications at the time of transactions are also strengthened.
  - The monitoring of transactions with countries judged to be highly risky and customers in the same countries is strengthened by focusing on prosecution cases and media reports on financial crime-related remittances, and the risk analyses and the corruption perception indexes (CPIs) conducted and created by foreign countries' authorities.
  - The periods of stay of foreign customers, such as international students and workers, is managed by a system after confirming their periods of stay in order to deal with risks, such as their accounts being sold when they return to their home countries.

In addition, efforts made by Japanese crypto-assets exchange service providers and the Financial Services Agency are introduced as good examples in the Guidance on Risk-based Supervision prepared by FATF and the Supervising Crypto-assets for Anti-money Laundering prepared by the Bank for International Settlements, etc.

D. Assessment of Risks

The important characteristics of crypto-assets are that its users are highly anonymous and the transfer of crypto-assets can be instantly executed across national borders. In addition, the regulation of crypto-assets differs from country to country. In light of these factors, if crypto-assets are misused for crimes, it is difficult to trace the transfer of the crypto-assets. Considering actual cases where the anonymity of crypto-assets was misused to convert illegally obtained crypto-assets into cash through a crypto-assets exchange service provider and remit the money to an account opened in another person's name, it is recognized that crypto-assets are at risk of being misused 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.

Furthermore, since the deposit-taking institutions are strengthening their AML/CFT countermeasures, there are people attempting to conduct ML/TF will use crypto-assets transactions in addition to goods and services handled by the deposit-taking institutions. 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.

[FATF Report on Crypto-assets]

In the "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing" published in September 2020, FATF described the points to observe and examples, etc. for private companies to verify if a transaction is suspicious. The main points to observe are as follows:

(1) Misuse of virtual currency exchange service providers based in countries where regulations on AML/CFT measures do not exist or are weak

(2) Quick transfer of virtual currencies to overseas virtual currency exchange service providers

(3) Misuse of multiple exchanges

(4) Use of anonymization methods (such as falsification of internet domain name or use of a tumbler, mixer,[*1] anonymous currencies (privacy coins), decentralized exchanges, etc.)

---

*1 Technology to make the connection with a transfer on a blockchain in which transactions are recorded by mixing transactions with transactions made by several other persons to integrate them and then redistributing them to each transferee. Anonymization service is called "mixer" and an intermediary of anonymization is called "tumbler," respectively.
See https://www.fsa.go.jp/policy/bgin/ResearchPaper_MRI_ja.pdf (3.2.1.1.2 Mixing).

(5) Cases where a victim is treated as a money mule (carrier) (e.g.: An offender transfers criminal proceeds to a bank account of the victim and later instructs the victim to purchase virtual currencies using that money.)

(6) Cases where an account is opened with a virtual currency exchange service provider by using a forged identification document.

In the report titled "Second 12-Month Review of Revised FATF Standards-Virtual Assets and VASPs" published in July 2021, quantitative market data regarding peer-to-peer (P2P) transactions[*1] of virtual currencies was presented for the first time. The data indicates that quite a large portion of virtual currencies transactions are P2P. As for the ratio of illegal transactions, the ratio of P2P transactions tends to be higher than transactions via virtual currency service providers, at least for direct transactions. However, due to data dispersion, it was not possible to determine the scale of market of the P2P sector or the scale of ML/TF risks related thereto. In the revised guidance on virtual currencies published by FATF in October 2021, FATF mentions the implementation of measures to identify, assess, and reduce risks when virtual currency exchange providers are involved with P2P transactions and warns the national government and business operators regarding the matter.

*1 Meaning transactions between individuals of crypto-assets, in which crypto-assets exchange service providers or other specified business operators that assume obligations related to AML/CFT measures are not involved.

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

A. Risk Factors

(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 27).

In recent years, the number of deposit-taking institutions 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.

Table 27 [Transactions by Foreign Currency Exchange Operators]

Year / Reporter		2018				2019				2020			
		Number of Reporters	Number of Transactions	Transaction Amount (million yen)	Transaction Amount for Each Transaction	Number of Reporters	Number of Transactions	Transaction Amount (million yen)	Transaction Amount for Each Transaction	Number of Reporters	Number of Transactions	Transaction Amount (million yen)	Transaction Amount for Each Transaction
Depository Institutions	Megabank (Note 2)	4	224,970	25,462	116,737	4	181,410	26,326	145,738	4	37,298	8,962	240,268
	Local Bank	92	185,578	11,969	64,613	88	183,687	10,554	57,653	81	39,687	3,706	93,392
	Shinkin Bank	120	4,222	398	95,023	110	3,716	326	88,446	85	718	74	102,808
	Foreign Bank	26	660	2,612	3,051,127	24	375	124	328,477	20	181	59	325,817
	Other (Note 3)	9	79,290	4,394	56,074	9	101,683	5,008	49,344	7	22,848	1,406	61,541
Businesses Other Than Depository Institutions	Funds Transfer Business/ Credit Card Business	14	202,066	12,707	62,622	15	230,404	14,952	65,065	6	39,767	3,148	79,168
	Hotel Business	42	3,538	393	91,286	34	2,813	161	58,883	23	559	39	69,192
	Travel Business	28	60,734	2,745	46,016	26	54,899	2,421	45,937	16	7,404	381	51,436
	Secondhand Articles Dealer Business	46	54,809	4,005	73,368	48	49,297	3,701	75,139	40	16,309	1,773	108,716
	Airport-related Business	5	153,773	5,099	33,161	6	154,056	5,377	35,283	3	26,592	998	37,511
	Large-scale Retail Business	3	344	9	24,928	2	230	6	25,949	2	54	2	40,373
	Other	126	90,680	15,586	168,613	64	109,611	34,756	355,879	60	45,136	20,607	456,563
Total		515	1,060,664	85,379	80,496	430	1,072,181	103,712	96,730	346	236,553	41,155	173,977

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: The Shinkin Central Bank, credit associations, Japan Post Bank, and other banks.

(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.
- Foreign-currency funds obtained in a robbery case in Japan were converted into Japanese yen
- A drug-trafficking organization used unregistered foreign-currency exchange operators to convert drug proceeds to foreign currency. (case in a foreign country)

B. Trends of STRs

The number of STRs submitted by foreign-currency exchange operators between 2018 and 2020 was 1,613.

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 (463 reports, 28.7%)
- Frequent buying and selling of foreign currency or traveler's checks in a short period of time (181 reports, 11.2%)
- When counterfeit currency, stolen currency, or suspected currency is received (73 cases, 4.5%)

C. Measures to Mitigate Risks

(a) Statutory measures

Many foreign-currency exchange operators in Japan are subject to business regulations related to their main business (i.e., they obtain a business license or are supervised by competent authorities). The Foreign Exchange Act requires foreign-currency exchange operators, whose transaction volume is more than 1 million yen in a month, to report to the Minister of Finance.

The Act on Prevention of Transfer of Criminal Proceeds requires foreign-currency exchange operators to conduct verification at the time of transactions, and to prepare and preserve verification records and transaction records when they make individual transactions of over 2 million yen.

In addition to the supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, the Foreign Exchange Act stipulates that the competent authorities may conduct on-site inspections of and issue a business improvement order to foreign-currency exchange operators if necessary.

(b) Measures by competent authorities

The Ministry of Finance has improved the Foreign Exchange Inspection Manual, which sets out points to note when developing internal control systems for verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds. In September 2018, the Ministry formulated the Foreign Exchange Inspection Guidelines, which explicitly adopt the risk-based approach. Furthermore, to ensure full compliance with laws and regulations by foreign-currency exchange operators, the Ministry of Finance has prepared a pamphlet outlining the reporting system, reporting procedures and the like for foreign-currency exchange operators, and has published the pamphlet on its website. Based on the results of on-site inspections and checking documents on compliance with laws and regulations and of risk control, the Ministry of Finance performs risk assessments on respective foreign-currency exchange operators from the perspectives of the scale of currency-exchange transactions, the internal control system, and the existence of non-face-to-face

transactions. Based on the results of such risk assessments, it also provides guidance and supervision corresponding to the risks.

As a result, it was discovered that many foreign-currency exchange operators do not prepare the documents that specified business operators need to prepare or simply use a standard or model form as is, or do not analyze their own transaction risks. For such foreign-currency exchange operators, the Ministry of Finance provides guidance during an on-site inspection so they will identify and assess their transaction risks. For foreign-currency exchange operators who do assess their risks to some degree, the Ministry verifies the extent to which they have implemented the risk-based approach from the perspective of whether appropriate risk assessment is conducted. The focus is on the transaction type, whether substantive risk mitigation measures have been taken in accordance with the Foreign Exchange Inspection Guidelines based on the abovementioned assessment, etc. If the Ministry detects inadequate implementation, it will provide guidance for the foreign-currency exchange operator. In July 2021, the Foreign Exchange Inspection Guidelines were revised to require foreign-currency exchange operators to: (1) prepare documents as specified business operators in light of the characteristics of their services, etc.; (2) continuously examine the information on customers with a frequency that corresponds to the risks of customers; (3) confirm the beneficial owners included in the information on customers by requesting reliable evidence; and (4) verify if a customer is a person subject to economic sanctions, etc.

Furthermore, the Ministry of Finance holds briefing sessions on obligations, etc. under the Act on Prevention of Transfer of Criminal Proceeds for foreign-currency exchange operators. In 2020, the Ministry of Finance dispatched its staff to briefings held by the Japan Ticket Association to explain the obligations of the currency exchange business under the Act on Prevention of Transfer of Criminal Proceeds. In addition, the Ministry together with the National Police Agency, sends them a document that requires full verification at the time of transactions and the creation of STRs. If compliance with the Act on Prevention of Transfer of Criminal Proceeds and the Foreign Exchange Act turned out to be insufficiently implemented during on-site inspection at the operators place of business, deficiencies will be pointed out and ordered to be improved.

So far, the Ministry of Finance has not issued rectification orders to foreign-currency exchange operators. However, when a case does arise showing that their verification at the time of transactions or its system of making STRs is insufficient, written or oral administrative guidance will be given, depending on the extent of the deficiencies.

These measures are important for keeping track of the actual state of foreign-currency exchange and to prevent foreign-currency exchange from being misused for ML/TF.

In light of the actual situation identified by the competent authorities, the key points to which foreign-currency exchange operators should pay attention are as follows:

- Management needs to play a leadership role with respect to AML/CFT measures.
- A system for appropriately conducting verification at the time of transaction needs to be established by setting up rules for implementing measures such as verification at the time of transaction.
- Appoint a manager (manager of verification at the time of transaction) responsible for the performance of verification at the time of transaction.
- The supervisor must correctly understand his obligations under the Act on Prevention of Transfer of Criminal Proceeds, even in small-scale foreign-currency exchange operators. A system needs to be established by setting up administrative rules and a written Risk Report Assessment by a Specified Business Operator, etc. so that no vulnerabilities exist in the entire internal control system pertaining to AML/CFT measures.
- Training must be provided to employees who are engaged in counter services.
- During internal audits or in-house inspections, including office work related to fulfillment of obligations, the implementation status of verification at the time of transaction, etc. needs to be subject to audits.
- When preparing a written Risk Report Assessment by a Specified Business Operator, etc., risk assessment, etc. needs to be conducted that takes into account characteristics of transactions dealt by the business operators, without just quoting standard templates as they are.
- The effectiveness of risk mitigation measures needs to be ensured so that risk assessment will not stay fragmented or abstract and that points of verification will not stay vague.

- Confirm a customer's identity, and purpose of transaction, etc., at the time of an exchange transaction exceeding the amount equivalent to 2 million yen. If the customer is a legal person, confirm the corporation's business content and verify the identity of the beneficial owner.
- Verifying the identity of not only the proxy, but also that of the actual customer.
- In the event of a currency exchange transaction involving a large amount of cash, in addition to the verification conducted at the time of transactions, check the source of cash and verify the authenticity of the transaction purpose, etc.
- If identity of customer is confirmed online in a non-face-to-face manner, properly record the image information and IC chip information provided by the customer.
- Spoofing transactions, fake transactions, transactions with Iran-North Korea resident customers, and transactions with foreign PEPs are transactions for which enhanced customer due diligence is required, which needs proper verification at the time of transaction.
- Judging whether transactions that are similar to ones found in the List of Reference Cases of Suspicious Transactions must be submitted as STRs.
- Performing enhanced CDD with respect to transactions with customers for which STRs were previously submitted.
- Appropriately recording reasons for determining that the transaction is not suspicious.

Regarding all foreign-currency exchange operators for which a deficiency has been detected, the competent authorities will request them to submit improvement measures, etc. as well as check the status of improvement through the next on-site inspection and a follow-up inspection, conducted as necessary.

(c) Measures by industry associations and business operator

Some industry associations, such as the Japan Ticket Association, which has many business members that handle foreign currency exchange, create and distribute documents prepared by specified business operators, etc. and manuals (templates) to develop internal regulations. Besides, they take voluntary AML/CFT measures against money laundering. 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. On the other hand, foreign-currency exchange operators who handle lower volumes tend to be modest in taking such measures.

The following are recognized as examples of efforts by foreign-currency exchange operators to implement the risk-based approach:

- Transactions for certain amounts are classified as high-risk transactions and, if such transactions occur, measures such as reports to the headquarters and execution of necessary research, etc. are specified in internal regulations.
- Mitigation measures with risks are taken by requesting customers to submit identification documents even for transaction in amounts that fall below the threshold for verification at the time of transaction, according to customer attributes.
- Principal identification documents are required to be submitted even for transactions with an amount lower than the threshold value of the law, for which collation is conducted with those who are subject to economic sanctions and foreign PEPs.
- Considering risks in which a large transaction is intentionally separated into two or more smaller transactions for the purpose of avoiding verification at the time of transaction, verification at the time of transaction is conducted based on a threshold value which is independently specified internally, and the results are saved into a database, and monitored to check whether there are any customers conducting transactions in large amounts in total.
- Continuous transactions are monitored with a built-in camera (taken with each transaction), in addition to setting a fixed amount of transaction limit per transaction in foreign currency with automatic change machine.
- Suspicious transactions are examined in order to submit STRs or not by analyzing transactions that were referenced by public institutions in the past, reflecting transactions and customer attributes of

types similar to any of those reflected in the transaction monitoring sheet, and branches report transactions falling under such types to the headquarters.

- For large transactions, a face-to-face verification at the time of transactions is conducted, and the date of purchase, purchasers (names of customers), and banknote serial numbers are recorded so that any person who is discovered later to have used counterfeit notes can be identified.

D. 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

A. Risk Factors

(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, 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.

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.

B. Trends of STRs

The number of STRs submitted by financial leasing operators between 2018 and 2020 was 615. 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.

- Transactions related to Boryokudan gangsters or their related parties (252 reports, 41.0%)
- Transactions related to financial leasing in which it was suspected that a lessee and a supplier conspired with the intent to defraud a financial leasing operator of money by pretending to install equipment (so called “empty leasing”) (128 reports, 20.8%)
- Transactions related to financial leasing in which it was suspected that a lessee etc., intended to defraud a financial leasing operator of money by concluding several leasing contracts based on the same facilities (so called “multiple leasing”) (61 reports, 9.9%)

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires financial leasing operators to conduct verification at the time of transactions, and to prepare and preserve verification records and transaction records when they conclude contracts. The Act also provides for supervisory measures by the competent authorities, such as requiring the submission of reports and conducting on-site inspections.

(b) Measures by competent authorities

The Ministry of Economy, Trade and Industry provides assistance, etc., to efforts by the following industry organizations to ensure financial leasing operators develop internal control systems.

(c) Measures by industry organization and business operator

The Japan Leasing Association and the Japan Automotive Leasing Association support AML/CFT measures taken by financial leasing operators. For example, they prepare and distribute leaflets and brochures to inform financial leasing operators of the outline of the Act on Prevention of Transfer of Criminal Proceeds and verification items at the time of transactions, and provide training.

The Japan Leasing Association conducts surveys on its members in writing, and conducts risk assessments of ML/TF based on the results of such surveys, etc. In addition, the Association investigates the parent

companies of its members, etc. to confirm that anti-social forces, etc. are not involved in the management of the members. The Japan Leasing Association has also developed guidelines on the performance of obligations under the Act on Prevention of Transfer of Criminal Proceeds and support provided by the Association. Furthermore, the Japan Leasing Association has been conducting a follow-up survey on its members' compliance with the internal guidelines since fiscal 2020 and is strengthening the training content.

The above guidelines were revised in July 2021 to clarify that such guidelines apply to the subsidiaries of members that are engaging in the financial leasing business (including overseas companies).

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 trainings 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.

D. 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

A. Risk Factors

(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 shop owner operating a loansharking business concluded a fictitious sale and purchase contract with a borrower in lieu of receiving repayment of a loan from the borrower, and transmitted a false sale and purchase information to a credit card issuing company and received the payment of the price.

B. Trends of STRs

The number of STRs submitted by credit card operators was 68,943 between 2018 and 2020.

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 (18,129 reports, 26.3%)
- Cases in which it was suspected that a person who was not a true card holder uses the credit card (16,533 reports, 24.0%)
- Transactions related to Boryokudan gangsters or their related parties (9,419 reports, 13.7%)

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires credit card operators to conduct verification at the time of transactions, and to prepare and preserve verification records and transaction records when they conclude contracts.

---

*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).

In addition to the supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, the Installment Sales Act stipulates that the competent authorities can order submission of reports, conduct on-site inspection, or issue business improvement orders to comprehensive credit purchase intermediaries if necessary for the enforcement of this Act. In addition, the Installment Sales Act stipulates that a system is required to ensure the fair and proper performance of the intermediation of comprehensive credit purchases in order to qualify for registration as a comprehensive credit purchase intermediary, and the review standard includes the establishment of a system for implementing measures stipulated in the Act on Prevention of Transfer of Criminal Proceeds. Furthermore, the Comprehensive Guidelines for Supervision of Comprehensive Credit Purchase Intermediaries includes matters to note regarding measures such as verification at the time of transaction under the Act on Prevention of Transfer of Criminal Proceeds and other measures listed in the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Credit Card Business.

(b) Measures by competent authorities

In addition, the Ministry of Economy, Trade and Industry clarified the basic concept of effective AML/CFT measures and, from the viewpoint of encouraging credit card business operators to implement effective measures, released the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Credit Card Business in August 2019, where credit card business operators are requested to establish and maintain risk management systems for ML/TF based on the Guidelines. In addition, the Ministry grasps the actual situation with regard to legal compliance and risk management through an on-site inspection, etc. and provide guidance and supervision, etc., corresponding to risks of respective credit card business operators.

In light of the actual situation identified by the competent authorities, the key points to which credit card operators should pay attention are as follows:

- Describing the name of a person for whom verification at the time of transaction has been conducted and the name, etc. of the author of verification records, as the ACT on Prevention of Transfer of Criminal Proceeds regulates to record them in verification records.
- Verifying the customer's identity via principal identification documents, etc. during verification at the time of transaction.
- Taking measures following the matters required to be addressed and matters expected to be addressed as described in the Anti-Money Laundering and Combating the Financing of Terrorism in the Credit Card Business.

The competent authorities have made improvements and corrections with respect to these matters by providing instructions, etc. to credit card operators.

(c) Measures by industry organization and business operator

The Japan Consumer Credit Association asks its members to conduct verification at the time of transaction and submit STRs by including these matters in its self-regulatory rules on STRs. 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 periodically meetings with law-enforcement authorities.

The following are recognized as examples of efforts by credit card operators to implement the risk-based approach:

- The increase in the credit limit of a credit card is not permitted in principle until one year has elapsed since the application, in order to mitigate the risks by a person attempting ML/TF using a contracted card.
- Transactions to purchase negotiable merchandise, such as gift certificates, during a short period are specified as high-risk transactions and, if such transactions are detected by a monitoring system, the credit card function is suspended, and a telephone call is made to the card holder to check the details of use or the user.

D. 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

A. Risk Factors

(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 Buildings Transaction Business Act (Act no. 176 of 1952). There were approximately 127,215 brokers as of the end of March 2021. In 2019, the annual amount of sales was about 45 trillion yen, and in 2020, the annual number of sales and purchase transactions that were registered 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)

B. Trends of STRs

The number of STRs submitted by real estate brokers was 21 between 2018 and 2020. 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, 42.9%)
- Unusual transactions or transactions related to customers who show unusual behavior or actions, based on the knowledge and experience of their own employees (4 reports, 19.0%)

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.

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds imposes on real estate brokers the obligations to conduct verifications at the time of transactions and to prepare and preserve verification records and transaction records when they conclude a sales contract for residential land or buildings or provide agency or intermediary services therefore.

Furthermore, in addition to the supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, the Real Estate Brokerage Act provides for supervisory measures by the competent authorities, such as requiring the submission of reports from, conducting on-site inspection of, and giving guidance and supervision to real estate brokers if necessary.

The Real Estate Brokerage Act also stipulates that every brokerage must keep books that record the names, addresses, etc., of customers who are counterparties of each sale, purchase, exchange or lease, or who ask agency service for such transactions for 5 years. These rules ensure proper and secure conduct of building-lot and building transactions.

(b) Measures by competent authorities

The Ministry of Land, Infrastructure, Transport and Tourism also checks documents or hold hearings to keep track of the actual status of compliance with laws and regulations and risk control by real estate brokers, and provides guidance, supervision, etc., corresponding to the risks of each real estate broker based on the information obtained through such research and orders.

In addition, the Ministry has established an industry-wide liaison council consisting of six real estate trading organizations to enhance the collaboration between related administrative organs and the real estate industry. The Ministry shares information each year via the Real Estate Business and Police Central Liaison Committee for Exclusion of Boryokudan, etc., to promote the elimination of anti-social forces such as Boryokudan gangsters from real estate transactions.

Furthermore, each regional development bureau and each prefectural government conducts on-site inspections of real estate brokers each year to examine the status of preparation of verification and transaction records that need to be prepared in accordance with the Act on Prevention of Transfer of Criminal Proceeds. They also provide programs on elimination of anti-social forces and AML/CFT measures under the Act on Prevention of Transfer of Criminal Proceeds, which are included in the lectures that are legally required to be taken when renewing a certificate of real estate transaction agent to be issued in accordance with the Real Estate Brokerage Act.

In light of the actual situation identified by the competent authorities, the points to which real estate brokers should pay attention are as follows:

- Verifying the customer's identity via principal identification documents, etc., during verification at the time of transaction.
- Describing the name of a person who conducts verification at the time of transaction and makes verification records, as the Act on Prevention of Transfer of Criminal Proceeds regulates to record them in verification records.
- Refer 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 trying to improve and correct these by giving guidance to real estate brokers.

(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 misuse for ML/TF and damage by anti-social forces, and distributes leaflets about announcements and education continuously. Furthermore, the council continuously follows the status of FATF's consideration of AML/CFT measures, exchange and share information among members of the council, and respond to FATF mutual evaluation of Japan.

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.

D. 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, fictious, 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

A. Risk Factors

(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 cannot be traced, so they are highly anonymous.

The Foreign Exchange Act and the Customs Act set forth the obligation to notify the customs in advance when exporting and importing precious metals[*1] that weigh more than one kilogram.

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 2019 administrative year,[*2] the number of processed cases (notifications and indictments) of gold smuggling was 199 (51% decrease compared to the previous accounting period), and the value of evaded taxes was about 360 million yen (63% decrease compared to the previous accounting period). The number of gold smuggling cases accounts for about 70% of all punished tax evasion offenses, including the evasion of customs duties (see Tables 29 and 30).

After the Ministry of Finance developed emergency countermeasures called “Stop Gold Smuggling” in 2017, strengthened the control over gold smuggling, and raised the punishment against gold smuggling substantially in 2018, the number of cases of gold smuggling has been decreasing. The modus operandi of smuggling has become advanced, and gold is being smuggled in small amounts. For example, offenders processed or transformed gold for smuggling in order to conceal it in body cavities, clothes, etc. Smuggling routes have diversified. Air passengers, air freight, international mail, etc. are used for smuggling. 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.

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.

---

*1 The precious metals stipulated in Article 6, paragraph 1, item 10 of the Foreign Exchange Act.

*2 The period from July 2019 to June 2020.

Table 28 Mechanism of Gold bullion Smuggling

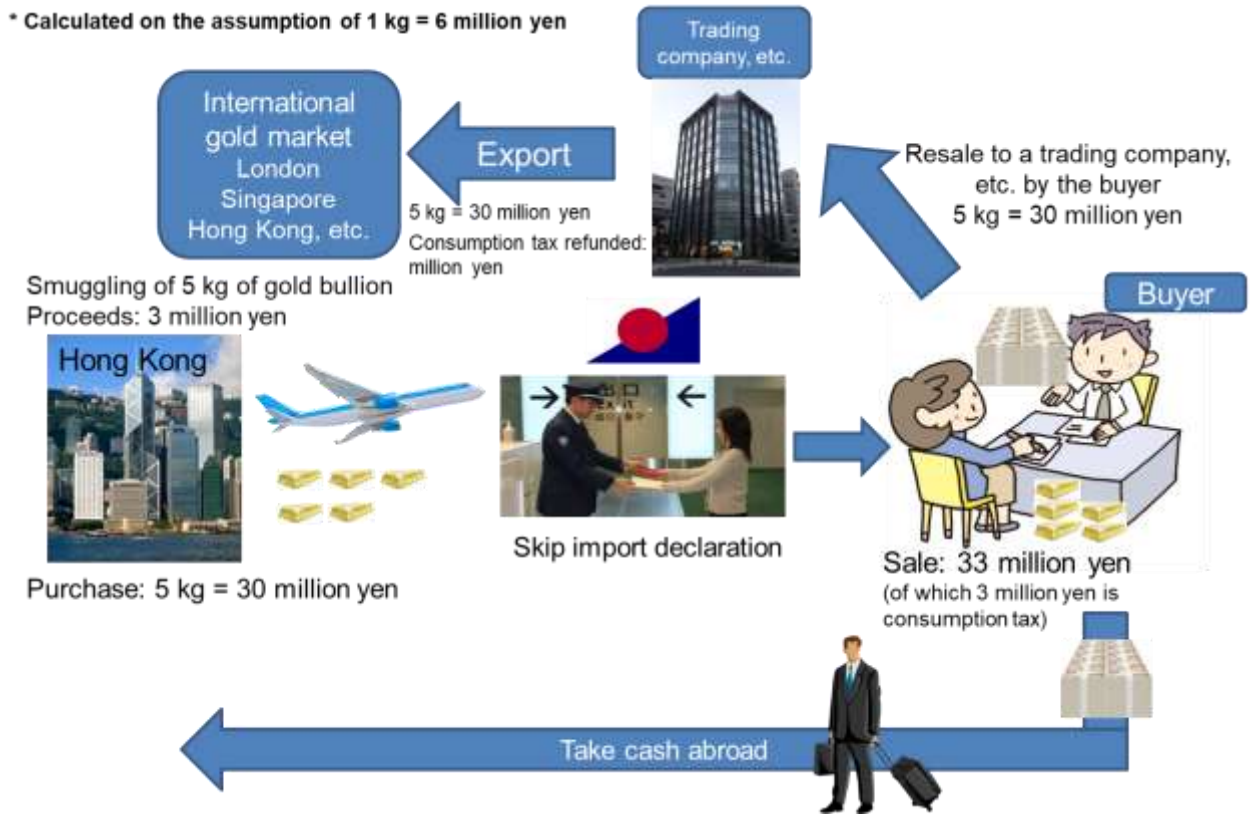


Table 29 Changes in the Number of Cleared Cases of Gold Bullion Smuggling

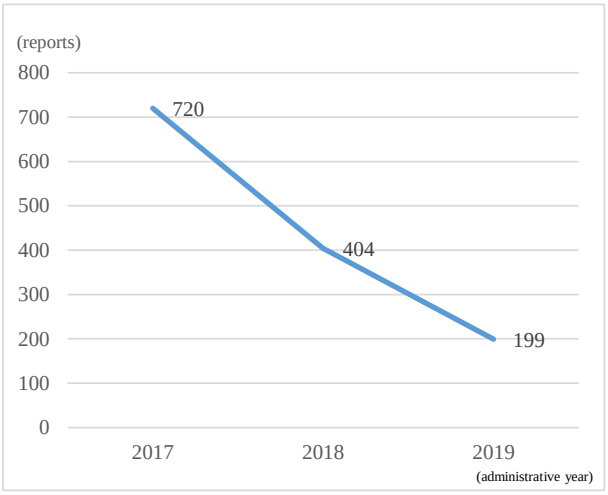
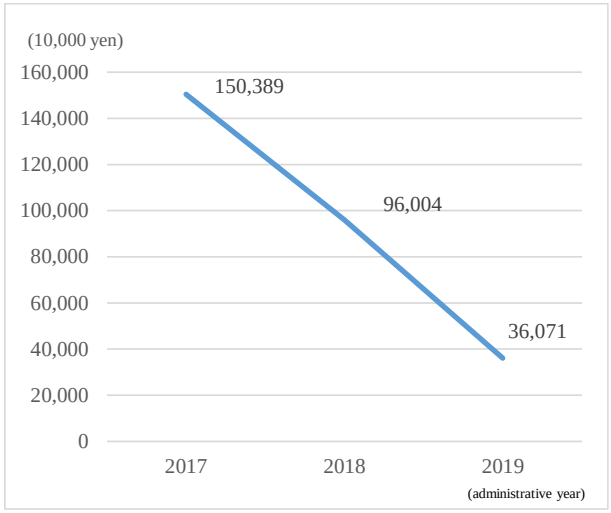


Table 30 Changes in the Amount of Evaded Taxes in the Cases of Gold Bullion Smuggling



(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 precious metals obtained through theft at a recycling shop by pretending to be another person.

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.

B. Trends of STRs

The number of STRs submitted by dealers in precious metals and stones was 1,232 between 2018 and 2020. 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 in a short period (819 reports, 66.5%)
- Purchases using large amounts of cash (115 reports, 9.3%)
- Frequent purchases in small amounts, resulting in a large amount of purchases (72 reports, 5.8%)

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires dealers in precious metals and stones to conduct verification at the time of transactions and prepare and preserve verification records and transaction records when they make sales contracts exceed 2 million yen in cash.

In addition to the supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, as for secondhand dealers and pawnbrokers that handle precious metals and stones, etc., the Secondhand Articles Dealer Act sets forth that police staff can conduct on-site inspections against secondhand dealers and that the prefectural public security commissions can order secondhand articles dealers to suspend their business as necessary. The Pawnbroker Business Act also sets forth that police officers can conduct on-site inspections against pawnbrokers and that the prefectural public security commissions can order pawnbrokers to suspend their business as necessary.

(b) Measures by competent authorities

The Ministry of Finance developed the Stop Gold Smuggling emergency countermeasures in November 2017 as a comprehensive countermeasure to strengthen inspection and punishment against the smuggling of gold bullion, and has been promoting various countermeasures under a cooperative system with relevant ministries and agencies, such as amendments to relevant laws and regulations. This includes requiring specified business operators that are involved in the logistics of gold bullion to thoroughly fulfil their obligations under the Act on Prevention of Transfer of Criminal Proceeds in order to ensure compliance in domestic logistics.

The Ministry of Economy, Trade and Industry performs documentary research and hearings to grasp the actual status of compliance with laws and regulations and risk control by dealers in precious metals and stones, and provides the guidance and supervision, etc., corresponding to risks faced by certain dealers in precious metals and stones based on information obtained through such research. Specifically, it was discovered that several gold bullion dealers had failed to submit STRs to the Minister of Economy, Trade and Industry even though they had repeatedly purchased gold bullion from the same customer with a large amount of cash. The Ministry of Economy, Trade and Industry gave administrative guidance to such gold bullion dealers in April 2018, April 2019, and July 2020. The summary of the administrative guidance is as follows:

- To submit STRs promptly
- To take measures to accurately perform their obligations, including conducting verifications at the time of transactions

The Ministry of Economy, Trade and Industry gives administrative guidance, including providing written guidance to gold bullion dealers that are considered to lack an understanding of risk management, etc.; holds information seminars for the industry; and provides an email address on its website to receive questions about

the Act on Prevention of Transfer of Criminal Proceeds from business operators. The Ministry is making efforts to ensure that business operators perform their obligations.

In addition, the Ministry explained about the compliance matters under the Act on Prevention of Transfer of Criminal Proceeds together with the Ministry of Finance at a workshop held by the Japan Gold Metal Association for its members in November 2019, and at a workshop for the jewelry dealers held with the Japan Jewelry Association in February 2020 together with the National Police Agency. In 2020, workshops were not held due to the Covid-19 pandemic, but the Ministry made efforts to enhance understanding of the Act on Prevention of Transfer of Criminal Proceeds by providing business operators with documents that summarized the compliance matters under the Act on Prevention of Transfer of Criminal Proceeds.

In light of the actual situation identified by competent authorities, the key points to which dealers in precious metals and stones should pay attention are as follows:

- If there is a suspicious transaction, businesses are obliged to notify the competent authorities.
- Strengthen education and training for employees and develop and review regulations to accurately perform verification at the time of transaction

Competent authorities are working to improve and correct the above by giving guidance to dealers in precious metals and stones.

(c) Measures by industry organization 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 makes efforts to ensure that its members understand the Act on Prevention of Transfer of Criminal Proceeds by distributing to its members posters, etc. supported by the Ministry of Economy, Trade and Industry to inform general consumers of the need to present their identification documents for gold bullion transactions; by advertising on its website; and by organizing workshops with employees of the Ministry of Economy, Trade and Industry and Ministry of Finance as lecturers for its members that are performing the actual work.

The Japan Jewelry Association makes efforts to ensure that business operators understand AML/CFT measures by preparing and distributing leaflets that describe the overview of the Act on Prevention of Transfer of Criminal Proceeds and the details of their obligations, holding seminars on AML/CFT measures, and updating the website designated for AML/CFT measures.

To promote initiatives for preventing ML/TF, industry organizations related to secondhand article dealings are communicating AML/CFT measures to all dealers in secondhand articles by creating manuals summarizing how they should perform their obligations under the Act on Prevention of Transfer of Criminal Proceeds and the Secondhand Articles Dealer Act and by holding training sessions.

The Japan Gold Metal Association and the Tokyo Pawn-Shop Cooperative are 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.

D. 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

A. Risk Factors

(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 specialized fraud, etc.

Based on the reports from prefectural police about suspected violations of the obligation to conduct verifications at the time of transactions and other reasons that were revealed during investigations related to specialized fraud, from 2018 through 2020, the National Public Safety Commission collected reports in accordance with the Act on Prevention of Transfer of Criminal Proceeds from postal receiving service provider. Specific violations identified through the submitted reports are as follows:

- Neglected to verify the customer's address.
- Neglected to check the customer's purpose of transactions.
- Neglected to check the customer's occupation or business details.
- Neglected to verify original identification documents at the time of face-to-face transactions.
- Neglected to record reasons for using a different name than the customer's.

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 specialized fraud through several locations including a postal receiving service provider.
- An offender caused repayments to a loan shark and proceeds derived from selling obscene DVDs to be sent to a postal receiving service provider with which a contract was concluded in another persons' name.

B. Trends of STRs

The number of STRs from postal receiving service providers between 2018 and 2020 was 12.

The Ministry of Economy, Trade and Industry revised and published the List of Reference Cases of Suspicious Transactions for postal receiving service by adding reference cases 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 (4 reports, 33.3%).

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.

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires postal receiving service providers to conduct verification at the time of transactions and prepare and preserve verification records and transaction records when they make service contracts. The Act on Prevention of Transfer of Criminal Proceeds also sets forth supervisory measures by competent authorities, such as requiring the submission of reports or documents and on-site inspections.

(b) Measures by competent authorities

The Ministry of Economy, Trade and Industry holds briefing sessions for postal receiving service providers in order to ensure thorough compliance with laws and regulations, explains the overview of the Act on Prevention of Transfer of Criminal Proceeds and points to be noted when they perform their obligations under the Act, distributes documents to postal receiving service providers to raise awareness about matters to be verified at the time of transactions, and posts explanations about the Act on its website.

Furthermore, the Ministry has summarized the actual conditions and issues of the postal receiving service industry and the risk of misuse for crimes. Simultaneously, the Ministry has formulated and published guidance for postal receiving service providers to introduce examples of efforts to prevent misuse for crimes. The website of the Ministry provides the latest information on the Act on Prevention of Transfer of Criminal Proceeds and useful information for strengthening countermeasures.

The Ministry makes efforts to ensure that the obligations under the Act on Prevention of Transfer of Criminal Proceeds are performed by conducting on-site inspections according to the Act, issuing rectification orders, and giving administrative guidance to business operators that violated their obligations to conduct verifications at the time of transactions, etc. During the period between 2018 to 2020, one rectification order was issued against a postal receiving service provider. The summary of the order is as follows:

- To provide in-house training on the Act on Prevention of Transfer of Criminal Proceeds and establish internal regulations in order to facilitate administrative procedures related to the Act on Prevention of Transfer of Criminal Proceeds
- To review work related to verification at the time of transaction and to prepare and preserve verification records

In addition, the Ministry checks documents and conducts surveys to keep track of the state of compliance with laws and regulations and risk control by postal receiving service providers. It also provides guidance, supervision, etc., corresponding to the risks of each postal receiving service provider based on the information obtained through such research and surveys, as well as from results of examining violation cases, etc.

In light of the actual situation identified by the competent authorities, the key points to which postal receiving service providers should pay attention are as follows:

- Establishing internal regulations, manuals, etc. for compliance with laws.
- Creating and saving verification records.
- Verifying the client's identity, the purpose of transaction, beneficiary owner, etc.
- Refer 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 have made improvements and corrections with respect to these matters by providing instructions, etc. to postal receiving service providers.

(c) Measures by business operators

The following are recognized as examples of efforts to implement the risk-based approach taken by postal receiving service providers:

- Information on transactions with customers that were 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.

D. 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

A. Risk Factors

(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 specialized fraud, etc.

The Ministry of Internal Affairs and Communications assesses that telephone receiving service providers that conduct non-face-to-face verification at the time of 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.

B. Trends of STRs

The number of STRs from telephone receiving service providers between 2018 and 2020 was none.

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires telephone receiving service providers to conduct verification at the time of transactions, and to prepare and preserve verification records and transaction records when they make service contracts. The Act on Prevention of Transfer of Criminal Proceeds also sets forth the supervisory measures by competent authorities, such as requiring the submission of reports or documents and on-site inspection.

(b) Measures by competent authorities

The Ministry of Internal Affairs and Communications holds briefing sessions for telephone receiving service providers in order to ensure their compliance with laws and regulations, explains the overview of the Act on Prevention of Transfer of Criminal Proceeds and points to be noted when they perform the obligations under the Act, and posts explanations about the Act on its website.

In March 2019, the Ministry held briefing sessions on the Act on Prevention of Transfer of Criminal Proceeds in Tokyo, Osaka, and Fukuoka for businesses providing telephone receiving services and telephone forwarding services.

In September 2019 and July 2020, the Ministry of Internal Affairs and Communications sent documents describing the overview of the Act on Prevention of Transfer of Criminal Proceeds and matters to be verified at the time of transactions to business operators providing telephone receiving or forwarding services as information that they should know as a specified business operator under the Act on Prevention of Transfer of Criminal Proceeds.

The Ministry also checks documents and conducts surveys to keep track of the actual state of compliance with laws and regulations and risk control by telephone receiving service providers, and provides guidance, supervision, etc., corresponding to the risks of each telephone receiving service provider based on the information.

In light of the actual situation identified by the competent authorities, the key points to which telephone receiving service providers should pay attention are as follows:

- Appropriately performing customer identification by receiving principal identification documents, etc.
- Creating and saving verification records
- 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 to make improvements and corrections with respect to these matters by providing instructions, etc. to telephone receiving service providers.

D. 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

A. Risk Factors

(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 2021, there were 857 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 specialized fraud and other crimes. These days, there are technologies available that allow telephone forwarding service providers that do not have the facilities or equipment necessary for telephone forwarding services to provide those services, so their customers can show a landline phone number (such as a phone number that starts with 03) through a cloud PBX 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. Specialized fraud cases use the telephone forwarding services of a provider that has purchased telephone lines from another company. This interferes with the investigation of specialized fraud cases because it takes time to verify the person who concluded the contract with the telephone forwarding service provider, who is the end client.

Actually, the number of reports from prefectural police to the National Public Safety Commission describing the use of telephone forwarding services for crimes including specialized fraud and suspected violations of the obligation by telephone forwarding service providers to conduct verifications at the time of transactions that were recognized have been increasing since 2017.

The National Public Safety Commission collected 27 reports in accordance with the Act on Prevention of Transfer of Criminal Proceeds during the period from 2018 to 2020. The details of major violations of obligations discovered as a result of collecting the reports in 2020 are as follows:

- Conducted verification at the time of transaction by accepting the presentation of an identification document that can be identified as a forged document.
- Neglected to verify the purpose of transactions, occupations of customers, etc.
- Failed to verify the identification data of a beneficial owner of a corporate customer.
- Failed to retain part of the verification records.

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 specialized fraud.

B. Trends of STRs

There were 14 STRs from telephone forwarding service providers between 2018 and 2020. 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 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 (4 reports, 28.6%).

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.

C. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires telephone forwarding service providers to conduct verification at the time of transactions, and to prepare and preserve verification records and transaction records when they make service contracts.

In addition to the supervisory measures based on the Act on Prevention of Transfer of Criminal Proceeds, the Telecommunications Business Act provides that the competent authorities may require the submission of reports from and conduct on-site inspection of telecommunication business operators as far as is necessary to enforce that Act.

(b) Measures by competent authorities

The Ministry of Internal Affairs and Communications holds briefing sessions for telephone forwarding service providers, explains the overview of the Act on Prevention of Transfer of Criminal Proceeds and points to be noted when they perform the obligations under the Act in order to ensure that the telephone forwarding service providers comply with the laws and regulations. In addition, the Ministry posts explanations about the Act on Prevention of Transfer of Criminal Proceeds on its website.

In March 2019, the Ministry held briefing sessions on the Act on Prevention of Transfer of Criminal Proceeds in Tokyo, Osaka, and Fukuoka for businesses providing telephone receiving or forwarding services. In September 2019 and July 2020, the Ministry sent a document describing the overview of the Act on Prevention of Transfer of Criminal Proceeds and matters to be verified at the time of transactions to business operators providing telephone receiving or forwarding services in order to share the information that they need to know as a business operator.

Furthermore, 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 2020, the Ministry issued a rectification order to three 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.

There was a case where a telephone forwarding service provider failed to comply with such rectification order issued by the Minister of Internal Affairs and Communications for the violation of the Act on Prevention of Transfer of Criminal Proceeds (violation of rectification order) and was arrested by the police (October 2020).

In addition, the Ministry conducts written surveys to keep track of the state of compliance with laws and regulations and risk control by telephone forwarding service providers. It also provides guidance, supervision, etc., corresponding to the risks of each telephone forwarding service provider based on the information obtained through such surveys, as well as from verification results related to violations, etc.

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 specialized fraud, etc. by giving guidance to them.

Offenders of specialized frauds 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.

D. 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 specialized fraud, etc.

Moreover, telephone forwarding service providers' neglect to fulfill their duties under laws and regulations as mentioned above due to deficiencies in their internal control systems 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 specialized frauds, 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, fictious, 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]

A. Risk Factors

(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 2021, 43,206 lawyers, 6 Okinawa special members, 445 foreign lawyers, 1,388 legal profession corporations and 9 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 Judicial Scriveners Associations (hereinafter referred to as "JFJSA"). As of the end of September 2021, 22,826 judicial scriveners and 913 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 2021, 49,480 administrative scriveners and 793 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 2021, 32,478 certified public accountants, 2 foreign certified public accountants, and 258 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 2021, 79,404 certified public tax accountants and 4,356 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.

---

*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.

(b) Typologies

The following cases are common examples of misusing legal/accounting services for money laundering:

- A loan shark asked a judicial scrivener to provide services for incorporation on its behalf, set up a shell company, deceived deposit-taking institutions to open accounts for the legal person, and misused the accounts to conceal criminal proceeds.
- An innocent certified public tax accountant and their corporation were used for bookkeeping of proceeds derived from fraud and gambling 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 transfer criminal proceeds.

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.

B. 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, he 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

JFBA analyzes the risks particular to legal practice via interviews with major law firms and from the contents of annual reports and others, and summarizes the results in the Risk Assessment of Money Laundering in Legal Practice (hereinafter, "Legal Practice Risk-NRA-FUR"). The JFBA publishes it in *Liberty and Justice*, the journal distributed to all its members and also, posts it on JFBA's website to encourage lawyers to understand the risks involved in legal practice. In the Legal Practice Risk-NRA-FUR, high-risk transactions refer to cash transactions, international transactions, legal persons without transparency of beneficial owner and others, which can be used for reference when lawyers conduct a risk assessment on their service. In addition, the March 2019 issue of "Liberty and Justice" published an article titled *Practicing the Risk-based Approach in Implementing Anti-Money Laundering Measures*, to introduce methods for identifying, assessing, and mitigating risks associated with legal practices and thereby to promote lawyers to implement a risk-based approach. In addition, JFBA supports the enhancement of measures implemented by each lawyer by preparing tools, FAQs, and e-learning programs to urge lawyers to comply with JFBA's regulations on AML/CFT measures and providing them to lawyers and bar associations, by posting examples of efforts made by law firms and the risk of money laundering associated with new technologies in its official magazine titled "Liberty and Justice," and by

sharing updates to public notices on international terrorists and points to note for identity verification during non-face-to-face transactions associated with the spread of Covid-19 on its member website.

In light of the actual situation identified by JFBA, lawyers should pay attention to the following matters for AML/CFT measures:

- Refer to the Risk Assessment of Money Laundering in Legal Practice 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.

Examples of lawyers' risk-based approaches include the following:

- A Japanese enterprise approached a law firm without introduction, requesting to make payments via the law firm and send money to foreign companies. The law firm rejected the request due to a high risk of money laundering after considering the fact that they were not familiar with the business details of the enterprise and other factors.
- When making decisions about whether to provide services for a certain client, lawyers identify, evaluate, and mitigate risks using credible published information (such as the register of legal persons, information published on the Internet, and asking the client) after confirming during the initial interview whether there is any property to be transferred, whether a proposed transaction is normal considering the business type of the client, and whether there is any financial difficulty or irregular point considering the business of the client or the other party to the proposed transaction, etc.
- When making decisions about whether to provide services for a certain client, lawyers use domestic and foreign databases to investigate whether the client is part of the anti-social forces or a foreign person who holds an important public position.
- Law firms have built an internal control system by creating and sharing internal regulations and manuals related to AML/CFT measures, organizing training and briefing sessions for lawyers and staff, and establishing responsible departments, such as internal control committees.
- Identification data is verified properly by specifying in engagement contract and advisory contract templates that the law firm can request identification documents from clients and that the clients should notify if there is a change in their identification data to promote cooperation from the clients.

b Japan Federation of Judicial Scriveners Associations (JFJSA)

JFJSA 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*. By creating training content and publishing it in the special training portal for its members in March and October 2019, and explaining the newly created reports on specific cases and referring to cases of suspicious transactions in judicial scriveners' services to its members in June of the same year, JFJSA again ensured that its members complied with the Guidelines for Conducting Duties to Prevent the Transfer of Criminal Proceeds.

According to the Articles of Association of the Judicial Scriveners, JFJSA has also required its members to submit a Report on Specific Cases (report on the status of compliance with the Act on Prevention of Transfer of Criminal Proceeds) since 2019. Accordingly, JFJSA monitors identity verifications and the preparation and retainment of transaction records, etc. (from July through December only in 2019 and January through December annually in and after 2020). Each Judicial Scriveners Association interviews its members who are recognized as being at risk based on the monitoring results and reports from members, and asks them to make corrections as necessary. JFJSA also decided to review and renew the questions and response methods for reports on specific cases in 2021.

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.

In April 2018, JFCAPLSA requested instructions from relevant ministries and agencies on AML/CFT measures and conducted a written survey with administrative scriveners nationwide on whether they conduct specified transactions, whether there are high-risk transactions, and whether they have refused specified transactions because the identity could not be verified and other matters related to the services of administrative scriveners under the Act on Prevention of Transfer of Criminal Proceeds.

Furthermore, since March 2019, JFCAPLSA has announced their obligations, such as the obligation to verify the identity and the obligation to prepare verification records on the website for administrative scriveners, in light of the survey results on the actual status of services of administrative scriveners under the Act on Prevention of Transfer of Criminal Proceeds. It has also posted explanations about the importance of preventing ML/TF, as well as statements to increase understanding and promote measures to prevent the involvement of crime groups and terrorist groups in advance.

In 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 the members of JICPA introduces e-learning trainings and publications related to ML/TF published by FATF. The April 2020 issue of the official magazine called "Accounting and Audit Journal" also carried an article titled "Basics and Risk-Based Approach of Countermeasures against Money Laundering and Terrorism by Accountants." JICPA also decided to hold seminars taught by external specialists for its members on the overview of the Act on Prevention of Transfer of Criminal Proceeds and the necessity of AML/CFT measures in 2021.

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.

Examples of certified public accountant or audit firm' risk-based approaches include the following:

- When concluding new contracts, risks are classified according to the business type of the other party. The higher the risk, the more documents are used to examine the contracts.
- When continuing audit contracts (which are renewed every year), the types of industries, officers, major shareholders, etc. are confirmed.
- When concluding new contracts for specific business categories, in-depth investigations are conducted based on past data.

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.

C. 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, fictious, 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.

2. Products and Services Utilizing New Technology that Require Further Examination of Actual State of Use, etc.

Products and Services Called Electronic Money[*1]

(1) Present Situation

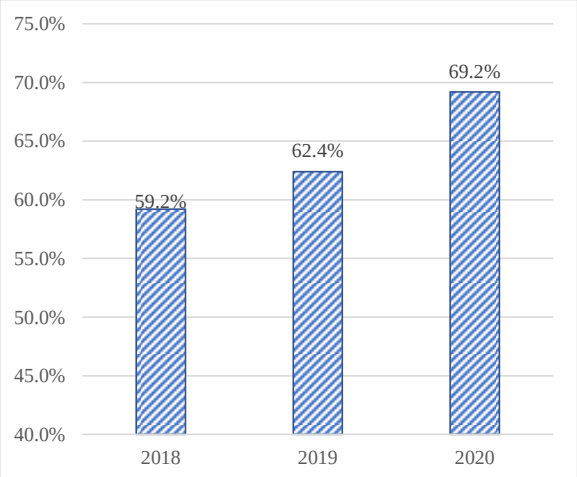
Prepaid payment instruments under the Payment Services Act refer to certificates, etc., or numbers, markings, or other signs (including instruments for recording the value in computer servers, etc.) that are issued in advance for the equivalent value, and used to purchase or lease goods or to receive services provided by the issuer, etc. Prepaid payment instruments are mainly used for specified services or at member shops for small-value payments. Many of the products and services called electronic money in Japan are prepaid payment instruments, which users generally use as prepaid-type electronic payment instruments by charging them in advance.

Prepaid payment instruments include own-business type, which is used for payment to issuers only, and third-party business type, which is used for payment at member shops, too. The Payment Services Act requires issuers of prepaid payment instruments for third-party business to be registered with the competent authorities and issuers of prepaid payment instruments for own business that have unused balances exceeding a designated threshold to notify to the competent authorities. The Act also sets many regulations, such as various reporting obligations, obligations to hold security deposits, management of member shops (measures to ensure that commodities are not against public order or morals), and the prohibition on refunding prepaid payment instruments in principle to ensure that prepaid payment instruments are properly managed.

In prepaid payment instruments, the monetary value is converted to an electromagnetic record and stored in an IC chip or servers on a network. Such instruments have excellent portability. Furthermore, in many cases, customers do not have to provide identification documents. Identity verification is often completed only with the customer's self-reported name, birth date, etc. upon issuance. These characteristics give prepaid payment instruments high anonymity, and in some cases, IC cards and other intermediaries can be transferred without difficulty.

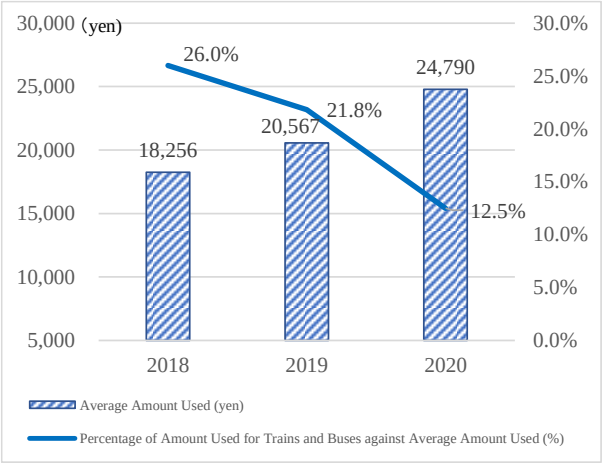
However, as refunds to holders of prepaid payment instruments are prohibited under the Payment Services Act, except cases where issuers discontinue business, users cannot freely withdraw funds with respect to the charge value[*2]. Furthermore, many issuers of prepaid payment instruments voluntarily set an upper limit for charging, and usage is limited to low-value payments at specified member shops.

Table 31 Households Possessing Electronic Money (Households of Two or More Persons)



Note: Data from the Ministry of Internal Affairs and Communications

Table 32 Average Amount of Electronic Money Used per Month by Households (Households of Two or More Persons)



Note: Data from the Ministry of Internal Affairs and Communications

---

*1 In this NRA-FUR, "electronic money" means monetary value equivalent to cash that is stored in a card, etc., and does not include credit cards, debit cards, post-pay, bus cards or other prepaid cards used for purchasing specific products or services.

*2 Business operators that issue prepaid payment instruments that can be used to withdraw or remit the amount stored in the card are considered to be funds transfer service providers, which are specified business operators under the Act on Prevention of Transfer of Criminal Proceeds. Therefore, they will assume the obligation to conduct verifications at the time of transactions when issuing such instruments.

(2) Typologies

The following cases are examples of misusing electronic money for money laundering:

- Electronic money obtained through fraud was sold via an online broker, and the paid money was remitted to an account opened in another person's name.
- An offender obtained the right to use electronic money through fraud and used it to purchase the right to use a different type of electronic money. The rights were resold to a purchaser who then remitted the payment to an account under another person's name, after which the money was withdrawn from an ATM.
- An offender made a successful bid for fictious goods put up for sale at an online auction site by pretending to be a fictious person, paid for the goods with electronic money in fictious transactions, and made the company operating the site transfer the price of the goods to an account managed by the offender as legal proceeds in order to cash electronic money obtained from fraud.
- A specialized fraud group colluding with a liquor distributor used electronic money obtained from fraud to purchase a large quantity of beer tickets, which are fictitiously put on sale by the liquor distributor on a shopping site, and made the company operating the site transfer the proceeds from the sale of the beer tickets to an account of the liquor distributor.
- Money obtained from specialized fraud was deposited to an account, cash was withdrawn to purchase electronic money gift cards, and the prepaid numbers of the gift cards were sent to a fraud group.
- A purchaser received the number of electronic money stolen from a victim by e-mail from a specialized fraud group and received the money.
- An offender recharged electronic money on a virtual prepaid card in another person's name created online using illegally obtained credit card information in order to pay for living expenses, etc., and also sent electronic money to a newly created virtual prepaid card in another person's name.

Of the 2,010 recognized cases of fraudulent billing fraud during 2020, 1,120 cases were conducted by the method of misusing electronic money, accounting for 55.7% of the total, and the amount of financial damage per case was approximately 890,000 yen. In the illegal remittance cases related to online banking that occurred in 2020, various modus operandi, such as purchase of crypto-assets or electronic money and recharging of prepaid cards, have been found, in addition to illegal remittance to deposit and savings accounts, which is a traditional type of modus operandi.

(3) Risk

Electronic money has a wide variety of forms and usages, but in general, they have excellent portability and high anonymity. In fact, there have been cases where electronic money was misused in the process of money laundering, and the number of such cases is on the rise. In Japan, however, refunds of prepaid payment instruments are prohibited under the Payment Services Act, so in principle, users cannot freely withdraw cash equivalent to the amount charged to a card. In addition, many issuers of electronic money have set a maximum amount of recharge now, and it can only be used at specific member stores, etc. However, coupled with the progress of cashless society, there are many stores where electronic money can be used, including online stores.

Furthermore, in line with the spread of electronic money, there have been cases of misusing electronic money for crimes. Some examples of misuse are as follows: (1) victims who were asked to pay usage fees to access fictitious paid sites, paid for with electronic money at convenience stores or other locations, were deceived into revealing their identities and were defrauded of money equivalent in value to the face value of the prepaid cards; (2) unauthorized access to smartphones and other mobile devices using bar codes or QR codes to illegally obtain credit card numbers, etc. in order to purchase goods.

Therefore, relevant ministries and agencies, business groups, etc. are conducting initiatives to raise awareness about the risk from the viewpoint of preventing not only money laundering crimes, but criminal damage in general. As specific initiatives, in August 2019, the Ministry of Economy, Trade and Industry, etc. requested business operators providing cashless payment functionality to put sufficient measures in place against unauthorized access, and the Payments Japan Association released the Guidelines for Preventing Unauthorized Use of Credit Card Numbers, etc. Improperly Leaked in Code Payments in April 2019. In addition, there are malicious traders engaging in the trade of electronic money usage rights aid despite knowing or suspecting that the electronic money was obtained through deception facilitate crimes or make crimes easy the police have enhanced their efforts to investigate the facts and dissolve such traders and have arrested cases of violation of the Act on Punishment of Organized Crimes and Control of Proceeds.

Furthermore, as a countermeasure against fraud in which electronic money is stolen, the police is promoting damage prevention in cooperation with related business operators, including convenience stores and companies issuing electronic money.

In light of these circumstances, it is necessary to keep monitoring the usage of electronic money in Japan.

[Casinos]

Casinos are legally operated in several countries and regions outside Japan. A report published by FATF in 2009[*1] pointed out the risk of money laundering stemming from casinos as follows:

- ○ Casinos are a cash intensive business, often operating 24 hours per day, with high volume of large cash transactions taking place very quickly.
- ○ Although casinos offer various financial services (accounts, remittance, foreign exchange, etc.), in some jurisdictions, casinos are regulated as entertainment venues, rather than financial institutions, and proper AML/CFT measures are not taken.
- ○ In some jurisdictions casino staff turnover is high, which can lead to poor education and training in AML/CFT measures.

Also, money laundering methods and techniques in casinos were mentioned as follows:

- ○ buying chips with criminal proceeds and then redeeming them for cash 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,

Considering the risk of casinos being misused for money laundering, the FATF Recommendations request casino business operators to verify the identity of customers and implement CDD measures when they establish continuous business relations with a customer or carry out financial transactions equal to or above USD/EUR 3,000. The FATF Recommendations also request that a license system be created for casinos to implement AML/CFT measures effectively.

In light of these requests, a license 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 include casino business operators as specified business operators, so casino business operators are required to verify customers at the time of transactions, prepare and preserve verification records and transaction records, submit STRs, etc. Furthermore, the Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds, which was amended by the Order for Enforcement of the IR Development Act (Order No. 72 of 2019, hereinafter referred to as the "IR Development Order") stipulates the following as specified transactions that require verifications to be conducted 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 addition to the regulations under the Act on Prevention of Transfer of Criminal Proceeds, the IR Development Act and IR Development Order impose the following obligations on casino business operators:

---

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

- To prepare the Regulations on Prevention of Transfer of Criminal Proceeds (examined by the Casino Regulatory Commission)
- To report to the Casino Regulatory Commission if the total amount involved in a transaction in which cash is received or refunded on one business day exceeds one million yen
- To take measures for preventing a customer from transferring chips to other persons, receiving chips from other persons, or taking them away from the casino gaming operation areas

In July 2021, the IR Development Act and IR Development Order were fully enacted, and the Ordinance for Enforcement of the Act for Development of Specified Integrated Resort Districts Related to Casino Regulatory Commission (Ordinance of Casino Regulatory Commission No. 1 of 2021) was enacted to create an environment in which casinos are not misused for money laundering.

Section 6. Low-risk Transactions

1. Factors that Mitigate Risks

In the light of customer types, transaction types, settlement methods, legal systems, etc., it is considered that the following transactions carry a low risk of misuse for ML/TF.

(i) Transactions that have a clear source of funds

When characteristics or ownership of a source of funds are clear, it is difficult to misuse them for ML/TF.

(ii) Transactions with the State or a local public entity

Transactions with the State 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) Transactions in which customers, etc. are limited by laws, 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) Transactions in which the process is supervised by the State, etc. based on laws, etc.

Transactions in which notification to or approval by the State etc. is required are supervised by the State, etc., so it is difficult to misuse them for ML/TF.

(v) Transactions in which 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) Transactions with minimal or no fund-accumulation features

Investment in products or services with no or minimal fund-accumulation features is inefficient for ML/TF.

(vii) Transactions below the regulatory threshold

Transactions below the regulatory threshold are inefficient for ML/TF. In the FATF Recommendations and Interpretative Notes etc., the FATF also sets out transaction amounts that are the thresholds for CDD measures.
Incidentally, 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.[*1]

(viii) Transactions in which 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 State, etc. Thus, customers' identities are clear and fund traceability is secured in such transactions.

---

*1 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. Low-risk Transactions

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

These transactions are prescribed by the current Ordinance as those for which simplified CDD is permitted, and provisions for them have been added to the following items. 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]

(1) Certain Transactions in Money Trusts, etc. (Article 4, paragraph 1, item 1 of the Ordinance)

Any transaction for the purpose of managing assets to be returned to a beneficiary (money trust) is provided for in Article 4, paragraph 1, item 1 of the Ordinance, and falls under transactions with factors to mitigate risks (i), (iii), (iv) and (viii). Therefore, they are deemed to present a low risk.

(2) Conclusion, etc. of Insurance Contracts (Article 4, paragraph 1, item 2 of the Ordinance)

The conclusion of insurance contracts set forth in Article 4, paragraph 1, item 2 of the Ordinance ((a) insurance contracts without payment of maturity insurance money etc., and (b) insurance contracts under which the total amount of refunds is less than 80% of the total amount of premiums paid) falls under transactions with factors that mitigate risks (vi). Therefore, they are deemed to present a low risk.

(3) Payment of Mature Insurance Money, etc. (Article 4, paragraph 1, item 3 of the Ordinance)

A. Payment of Mature Insurance Claims, etc. for Insurance Contracts whose Total Repayment is less than the Total Premium

Payment of mature insurance money, etc. of insurance contracts for which total repayment is under 80% of total premium, prescribed in Article 4, paragraph 1, item 3, (a) of the Ordinance, falls under transactions with factors to mitigate risks (vi). Therefore, they are deemed to present a low risk.

B. Payment of Mature Insurance Claims, etc. for Qualified Retirement Pension Contracts, Group Insurance Contracts, etc.

Payment for mature insurance claims, etc. for qualified retirement pension contracts or group insurance contracts[*2] as prescribed in Article 4, paragraph 1, item 3, (b) of the Ordinance, falls under the transactions with factors to mitigate risks (i), (iii), (iv) and (viii). Therefore, they are deemed to present a low risk.

(4) Transactions Carried out in a Securities Market, etc. (Article 4, paragraph 1, item 4 of the Ordinance)

Buying and selling of securities carried out in a securities market, etc.,[*3] as prescribed in Article 4, paragraph 1, item 4 of the Ordinance, fall under transactions with factors to mitigate risks (iii) and (viii). Therefore, they are deemed to present a low risk.

(5) Transactions of Government Bonds, etc. that are Settled by an Account Transfer at the Bank of Japan (Article 4, paragraph 1, item 5 of the Ordinance)

Transactions of government bonds, etc. that are settled by an account transfer at the Bank of Japan, prescribed in Article 4, paragraph 1, item 5 of the Ordinance, fall under transactions with factors to mitigate risks (iii) and (viii). Therefore, they are deemed to present a low risk.

---

*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.

(6) Certain Transactions concerning the Loan of Money, etc. (Article 4, paragraph 1, item 6 of the Ordinance)

A. Loans for Which Settlement is Made by an Account Transfer at the Bank of Japan

Loans for which settlement is made by an account transfer at the Bank of Japan, as prescribed in Article 4, paragraph 1, item 6, (a) of the Ordinance, fall under transactions with factors to mitigate risks (iii) and (viii). Therefore, they are deemed to present a low risk.

B. Loans, etc. Based on Insurance Contracts etc. for which Total Repayment is Less Than the Total Premium

Loans, etc. based on insurance contracts etc. for which total repayment is under 80% of the total premium, as prescribed in Article 4, paragraph 1, item 6, Insurance (b) of the Ordinance, fall under transactions with factors to mitigate risks (i), (iii), (iv) and (vi). Therefore, they are deemed to present a low risk.

C. Individual Credit

Individual credit*1 as prescribed in Article 4, paragraph 1, item 6, (c) of the Ordinance etc., falls under the transactions with factors to mitigate risks (viii). Therefore, it is deemed to be low-risk.

(7) Certain Transactions in Cash Transactions, etc. (Article 4, paragraph 1, item 7 of the Ordinance)

A. Transactions in Which a Public or Corporate Bearer Bond is Provided as a Mortgage

Transactions in which a certificate or coupon of a public or corporate bearer bond that exceeds 2 million yen is provided as a mortgage, prescribed in Article 4, paragraph 1, item 7, (a) of the Ordinance, fall under transactions with factors to mitigate risks (i) and (viii). Therefore, they are deemed to present a low risk.

B. Payment or Delivery of Money and Goods to the State or a Local Public Entity

Payment or delivery of money and goods to the State or a local public entity, prescribed in Article 4, paragraph 1, item 7, (b) of the Ordinance, fall under transactions with factors to mitigate risks (viii). Therefore, they are deemed to present a low risk.

C. Payment of Utility Charges

Payment of electricity, gas or water charges, prescribed in Article 4, paragraph 1, item 7, (c) of the Ordinance, falls under transactions with factors to mitigate risks (viii). Therefore, they are deemed to present a low risk.

D. Payment of School Entrance Fees, School Fees, etc.

Payments of entrance fees, school fees, etc. for an elementary school, a junior high school, a high school, a university, etc., as prescribed in Article 4, paragraph 1, item 7, (d) of the Ordinance, fall under transactions with factors to mitigate risks (viii). Therefore, they are deemed to present a low risk.

E. Exchange Transactions, etc. Carried out for Accepting or Refunding Deposits or Savings

Exchange transactions, etc. for accepting or refunding deposit/savings not more than 2 million yen, as prescribed in Article 4, paragraph 1, item 7, (e) of the Ordinance, fall under transactions with factors to mitigate risks (vii) and (viii). Therefore, they are deemed to present a low risk.

F. Receipt and Payment for Goods in Cash with Measures Equivalent to CDD, Including Verification at the Time of Transaction

Receipt and payment for goods in cash not more than 2 million yen that accompany an exchange transaction, and in which the payment receiver conducted verification at the time of transaction similar to the case for specified business operators, prescribed in Article 4, paragraph 1, item 7, falls under transactions with factors to mitigate risks (vii) and (viii). Therefore, they are deemed to present a low risk.

---

*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.

(8) Opening a Special Account under the Act on Book-Entry Transfer of Corporate Bonds and Shares (Article 4, paragraph 1, item 8 of the Ordinance)

Opening a special account under the Act on Transfer of Bonds, Shares, etc., prescribed in Article 4, paragraph 1, item 8 of the Ordinance, falls under transactions with factors to mitigate risks (iii) and (viii). Therefore, they are deemed to present a low risk.

(9) Transactions through SWIFT (Article 4, paragraph 1, item 9 of the Ordinance)

Transactions in which verification is made or settlement among specified business operators is directed through SWIFT[*1], prescribed in Article 4, paragraph 1, item 9 of the Ordinance, falls under transactions with factors to mitigate risks (iii) and (viii). Therefore, they are deemed to present a low risk.

Note that, as described in the part titled "International Transactions" of *Section 4 Risk of Transaction Types, Countries/Regions, and Customer Attributes* of this NRA-FUR, international foreign-exchange transactions are high-risk transactions.

(10) Specified Transactions in Financial Leasing Contracts (Article 4, paragraph 1, item 10 of the Ordinance)

Financial leasing transactions in which the rental fee received in one instance by a lessor from a person who receives leasing services is 100,000 yen or less, as prescribed in Article 4, paragraph 1, item 10 of the Ordinance, fall under transactions with factors to mitigate risks (vii). Therefore, they are deemed to present a low risk.

(11) Buying and Selling Precious Metals and Stones, etc. in Which the Payment is Made through Methods Other Than Cash (Article 4, paragraph 1, item 11 of the Ordinance)

Transactions involving precious metals and stones, etc. in which the payment is over 2 million yen and is made through methods other than cash, as prescribed in Article 4, paragraph 1, item 11 of the Ordinance, fall under transactions with factors to mitigate risks (viii). Therefore, they are deemed to present a low risk.

(12) Certain Transactions in Telephone Receiving Services (Article 4, paragraph 1, item 12 of the Ordinance)

Certain transactions concerning telephone receiving services prescribed in Article 4, paragraph 1, item 12 of the Ordinance ((a) service contracts for telephone receiving services, under which the provision of telephone receiving services is indicated to a third party, and (b) contracts for a call center business, etc.[*2]) fall under transactions with factors that mitigate risks (v). Therefore, they are deemed to present a low risk.

(13) Transactions with the State, etc. (Article 4, paragraph 1, item 13 of the Ordinance)

A. Transactions That the State etc. Conducts Based on Statutory Authority

Transactions that the State or a local public entity conducts based on statutory authority, prescribed in Article 4, paragraph 1, item 13, (a) of the Ordinance, fall under transactions with factors to mitigate risks (i), (ii), (iii), (iv) and (viii). Therefore, they are deemed to present a low risk.

---

*1 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.

*2 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.

B. Transactions That a Bankruptcy Trustee, etc. Conducts Based on Statutory Authority

Transactions conducted by a bankruptcy trustee, prescribed in Article 4, paragraph 1, item 13, (b) of the Ordinance, fall under transactions with factors to mitigate risks (i), (iii), (iv) and (viii). Therefore, they are deemed to present a low risk.

C. Transactions Performed by Specified Business Operators with Their Subsidiaries as Customer, etc.

Transactions performed by specified business operators with their subsidiaries as customers, etc. set forth in Article 4, paragraph 1, item 13, (c) of the Ordinance fall under transactions with factors that mitigate risks (i) and (viii). Therefore, they are deemed to present a low risk.

(14) Certain Transactions in Agent Work, etc. for Specified Mandated Acts by Judicial Scriveners, etc.[*1] (Article 4, paragraph 3 of the Ordinance)

A. Conclusion of a Voluntary Guardianship Contract

Conclusion of a voluntary guardianship contract, prescribed in Article 4, paragraph 3, item 1 of the Ordinance, falls under transactions with factors to mitigate risks (iv) and (viii). Therefore, it is deemed to present a low risk.

B. Transactions That the State, etc. Conducts Based on Statutory Authority

Transactions conducted by the State, etc. and a bankruptcy trustee, etc. based on statutory authority, prescribed in Article 4, paragraph 3, item 2 of the Ordinance, fall under transactions with factors to mitigate risks (i), (iv) and (viii), and also (ii) or (iii). Therefore, they are deemed to present a low risk.

---

*1 Regarding agent work, etc. for specified mandated acts pertaining to the management or disposition of property listed in item 3 of the middle column of the row of persons listed in Article 2, paragraph 2, item 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

In light of the results of the assessment presented in this NRA-FUR, competent authorities need to continue to make sure that specified business operators comply with the obligations under the laws and regulations, to identify and understand ML/TF risks associated with their supervising business operators, and to provide further guidance and conduct supervision on a risk-based approach. Particularly for business operators whose efforts in AML/CFT at lower level, competent authorities need to provide guidance and conduct supervision properly. In parallel, for those business operators, competent authorities need to share the information including good practices for AML/CFT compliance in collaboration with industry associations in order to improve the level of AML/CFT measures of the whole industry of complying with the requirements such as suspicious transaction reporting and establishing appropriate internal AML/CFT mechanism. Competent authorities should also continue their efforts of monitoring business operators' compliance of AML/CFT requirements.

Specified business operators need to comply with their obligations under the laws and regulations as a matter of course. Moreover, not only simply verifying whether there is a violation of laws and regulations, but also business operators need to identify the risks they face and take appropriate measures such as reporting of suspicious transaction by taking into account the characteristics of their businesses and risks associated therewith comprehensively and concretely. In particular, for products and services that are at a relatively higher or increasing risk of misuse for ML/TF than other business categories, substantial AML/CFT measures need to be implemented to mitigate individual risk properly.

Taking the opportunity of the publication of the FATF Fourth Round of Mutual Evaluation Report of Japan, in August 2021, the Government of Japan established the "Inter-Ministerial Council for AML/CFT/CPF Policy" jointly chaired by the National Police Agency and the Ministry of Finance in order to strongly advance the Government's measures as a whole. At the same time, the Government of Japan formulated and released the AML/CFT/CPF Action Plan for the next three years. This action plan aims to improve legislative framework and the implementation of AML/CFT/CPF measures. Specifically, for example, the action plan lists the following action items: renewing the National Risk Assessment, strengthening supervision of AML/CFT/CPF measures taken by specified business operators, enhancing transparency of beneficial ownership information, establishment of a task force to improve the prosecution rate for money laundering offenses, enhancing ML investigation and prosecution and increasing the prosecution rate of ML cases with the efforts including the establishment of the task force, and prevention from abusing the NPO sector. It is important to ensure that the action plan will be implemented steadily while taking into account the risks identified in the national risk assessment reports. Furthermore, to work steadily on necessary legislative actions, the Government of Japan established the Office for Legislative Responses to the FATF Recommendations in the Cabinet Secretariat.

To further promote AML/CFT measures nationwide, competent authorities and specified business operators need to collaborate to raise public awareness on AML/CFT measures, get understanding on the importance of the measures, and obtain cooperation of specified business operators. To this end, competent authorities and specified business operators need to continuously and strongly promote the outreach to the citizens by employing various tools.

It is expected that financial flows of criminal proceeds and terrorism financing will be diversified as globalization of the economic activities and the development of new technologies go on in the future. It is critical for competent authorities and specified business operators to fully understand their roles mentioned above and make efforts to implement AML/CFT measures in cooperation with one another by taking into account the risks presented in this report and domestic/global trends, in order to prevent the transfer of criminal proceeds and terrorism financing effectively, continue to secure the safety and peace of citizens, and contribute to the sound economic development.