Tentative Translation

November 2020

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)
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 Crime	Act on Punishment of Organized Crime and Control of Crime Proceeds (Act No. 136 of 1999)
Act on Punishment of Terrorist Financing	Act on Punishment of Financing to Offences of Public Intimidation (Act No. 67 of 2002)
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)

[List of Main Contents of the 2020 NRA-FUR]

Environment surrounding Japan		(1) Geographic Environment (2) Social Environment (3) Economic Environment (4) Criminal Circumstances, etc.
Analysis of money laundering offences, etc.		(1) Offenders (Boryokudan, specialized fraud groups, and crime groups of foreigners in Japan) (2) Predicate Offences (theft, fraud, violation of the Investment Act or the Money Lending Business Act, computer fraud, habitual gambling/running a gambling place for profit, violation of the Amusement Business Act, violation of the Anti-Prostitution Act, etc.)
High-Risk Transactions	Transaction types	(1) Non-face-to-face Transactions (2) Cash Transactions (3) International Transactions
	Countries/ regions	Countries/regions pointed out as having deficiencies in their AML/CFT systems or controls in the FATF Public Statement: Iran and North Korea (This item reflects the FATF Public Statement, and the countries/regions regarded as factors change according to the Statement.)
	Customer attributes	(1) Anti-social Forces (Boryokudan, etc.) (2) International Terrorists (Islamic Extremist Groups, etc.) (3) Non-resident Customers (4) Foreign Politically Exposed Persons (5) Legal Persons without Transparency of Beneficial owner
Products/services considered to present risks		(1) Products/Services Dealt with by Deposit-taking Institutions (deposit/savings accounts, deposit transactions, domestic exchange transactions, safe-deposit boxes, bills/checks) (2) Insurance Dealt with by Insurance Companies, etc. (3) Investment Dealt with by Financial Instruments Business Operators, etc. and Commodity Derivatives Business Operators (4) Trusts Dealt with by Trust Companies, etc. (5) Money Lending Dealt with by Money Lenders, etc. (6) Fund Transfer Services Dealt with by Fund Transfer Service Providers (7) Crypto-assets Dealt with by Crypto-assets Exchange Service Providers (8) Foreign Currency Exchanges Dealt with by Currency Exchange Operators (9) Financial Leasing Dealt with by Financial Leasing Operators (10) Credit Cards Dealt with by Credit Card Operators (11) Real Estate Dealt with by Real Estate Brokers (12) Precious Metals and Stones Dealt with by Dealers in Precious Metals and Stones (13) Postal Receiving Services Dealt with by Postal Receiving Service Providers (14) Telephone Receiving Services Dealt with by Telephone Receiving Service Providers (15) Telephone Forwarding Services Dealt with by Telephone Forwarding Service Providers (16) Legal/Accounting Services Dealt with by Legal/Accounting Professionals
Low-risk transactions	Factors	(1) The Source of Funds is Clear (2) The National or Local Governments are Customers, etc. (3) Customers are Limited by Laws and Regulations, etc. (4) The Transaction Process is Supervised by the National Government, etc. via Laws and Regulations (5) It is Difficult to Disguise the Actual Status of Legal Persons, etc. (6) Fund Accumulation Features are Low or Absent (7) Transaction Amounts are Below the Regulation Threshold (8) Customer Identification Methods are Secured by Laws, Regulations, etc.
	Transactions	Transactions for which simplified CDD is permitted, prescribed in Article 4 of the Ordinance (note, however, that simplified CDD is not allowed in the case of suspicious transactions, etc.)
Products/services using new technology		Electronic money

Section 1. Overview of Risk Assessment

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 business operators, in keeping with the contents of the NRA-Baseline Analysis. [*5]

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 Recommendation request business operators to take appropriate steps to identify and assess ML/TF risks with respect to their products and services to implement 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, applying risk-based approach (e.g. applying enhanced CDD to the higher risk transactions) is effective. As a prerequisite, specified business operators need to accurately understand the risks inherent in the transactions they carry out. Accordingly, it has been decided that the National Public Safety Commission, which is in a position to gather, arrange, and analyze information relating to the transfer of criminal proceeds or concerning suspicious transactions, is to prepare and publish an NRA-FUR describing the risks for each category of transaction carried out by business operators. Expert

---

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

*2 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 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 in this NRA-FUR include terrorist financing risks.

knowledge and information are to be 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. On October 1, 2016, Japan enforced the revised Act on Prevention of Transfer of Criminal Proceeds, Enforcement Order and Ordinance which stipulates the methods for making decisions about reporting suspicious transactions and the obligation for specified business operators to take measures for accurately performing verification at the time of transaction, etc. while taking into consideration the contents of the NRA-FUR.

Specified business operators are required to implement appropriate measures based on the abovementioned revised Act in order to prevent the transactions from being misused for ML/TF. Specifically, specified business operators are required to understand and take into account the contents of the NRA-FUR (Sections 1 to 5) relating to the transactions, etc. they handle. They also need to pay attention in their justification on why those transactions 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.

Moreover, the Act on Prevention of Transfer of Criminal Proceeds and the Ordinance call on specified business operators to apply the risk-based approach based on the risk assessment conducted in this manner. This is in order to properly conduct verification at the time of transaction commensurate with the risk level of their own transactions.

The table below shows revisions made in the Act to address the identified ML/TF risks and other relevant legal obligations to properly conduct verification at the time of transaction, etc.

[Revisions to the Act to address ML/TF risks]

○ Revisions to the Act on Prevention of Transfer of Criminal Proceeds, etc. enforced on October 1, 2016

• Clarification of methods for making decisions about suspicious transaction reports (STRs)

Specified business operators (excluding judicial scriveners, etc.) should decide on whether to file STRs by considering the contents of the NRA-FUR and the methods prescribed by a governing Ordinance (including a comparison with the modes of ordinary transactions related to the specified business) in addition to the results of verification at the time of transaction, the modes of the transactions in question, or other circumstances.

• Obligation to verify at the time of concluding correspondence contracts*[1]

Specified business operators who carry out exchange transactions as businesses may enter correspondent banking relationships with exchange transaction business operators located in foreign countries. In such cases, they should verify that these operators abroad have developed systems necessary for accurately implementing the measures equivalent to verification at the time of transaction, and so forth.

• Implementation of enhanced customer due diligence (CDD) at the time of transaction with foreign PEPs

Specified transactions with foreign politically exposed persons (PEPs) should be added to the list of transactions subject to enhanced CDD at the time of transaction.

• Obligation to identify beneficial owners

Identification of natural persons who ultimately own or control legal persons or legal arrangements through their voting rights or other means should be verified as the beneficial owner of the legal persons or legal arrangements.

• Customer identification methods involving identification documents without photographs

When customer identification documents without photographs, such as health insurance cards or pension books, are used, aside from the presentation of these documents, additional measures should be required, like sending transaction-related documents to the home addresses of customers, etc., as a postal item that is not to be forwarded.

• Implementation of verification for transactions divided into multiple transactions below threshold values to avoid exceeding the threshold for a single transaction

It may be immediately evident that a single transaction is divided into multiple transactions below the threshold to reduce each transaction's transaction amount. In that case, they should be regarded as a single transaction.

---

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

○ Revisions to the Act on Prevention of Transfer of Criminal Proceeds enforced on April 1, 2017

Virtual currency (crypto-assets) exchange service providers are added to specified business operators.

○ Revisions to the Act on Prevention of Transfer of Criminal Proceeds promulgated on July 27, 2018 (unenforced)

Casino business operators are added to specified business operators.

○ Revisions to the Ordinance promulgated on November 30, 2018

For FinTech support, a new mechanism has been established to complete online customer identification (enforced on November 30, 2018). Also, more rigorous identification methods have been applied in case postal item that is not to be forwarded is used in non-face-to-face transactions (enforced on April 1, 2020).

○ Revisions to the Act on Prevention of Transfer of Criminal Proceeds enforced on May 1, 2020

The term "virtual currency" prescribed in the Act on Prevention of Transfer of Criminal Proceeds was revised to "crypto-assets." Furthermore, "crypto-assets exchange service providers" who manage crypto-assets for others without exchanging crypto-assets, etc., as businesses are also added to specified business operators.

[Legal Obligations Imposed on Specified Business Operators]

The Act on Prevention of Transfer of Criminal Proceeds, and its Enforcement Order and Ordinance, oblige specified business operators to perform verification at the time of specified transactions (Article 4 of the Act on Prevention of Transfer of Criminal Proceeds), prepare and store verification records, etc. (Article 6 of the same Act), prepare and store transaction records, etc. (Article 7 of the same Act), and file suspicious transaction reports (STRs) when the assets received in such transactions are suspected to be criminal proceeds or when customers, etc. are suspected of committing acts amounting to the concealment of criminal proceeds, etc. (Article 8 of the same Act).

[Risk Control by Specified Business Operators (Developing Internal Systems Based on the Risk-based Approach)]

The revised Act on Prevention of Transfer of Criminal Proceeds enforced on October 1, 2016, and its Enforcement Order and Ordinance, stipulate that specified business operators shall strive to take the following measures to accurately perform verification at the time of transaction, etc.:

○ Implement employee education and training

○ Prepare internal rules for implementing measures, including verification at the time of transaction

○ Appoint a general manager responsible for audits and other operations required for accurate implementation of measures, including verification at the time of transaction

○ Other measures that should be taken, in consideration of the contents of the NRA-FUR, as prescribed by the Ordinance (Article 11 of the same Act)

The Ordinance prescribes the following measures:

○ Implement specified business operators' own risk assessments (including "the document prepared by specified business operators", etc.)

○ Collect, arrange, and analyze information necessary for taking measures, including verification at the time of transaction, etc.

○ Continuously scrutinize the verification and transaction records stored

○ Receive approval from the general manager on high-risk transactions (*)

○ Take necessary measures to recruit staff with skills required to accurately implement measures, including verification at the time of transaction

○ Conduct audits required to accurately implement measures, including verification at the time of transaction (Article 32 of the Ordinance)

(*) The following are high-risk transactions:

○ Transactions prescribed in the first sentence of paragraph 2 of Article 4 of the Act on Prevention of Transfer of Criminal Proceeds (transactions with a party suspected of pretending to be a customer, etc. or representative person, etc. related to the verification performed at the time of another relevant transaction; transactions with a customer who is suspected of having presented false information concerning the matters subject to verification at the time of another relevant transaction; transactions with persons who reside or are located in countries or regions whose AML/CFT systems are not considered sufficiently developed; and transactions with persons who occupy important positions in foreign governments, etc.)

○ Transactions requiring special attention in customer due diligence (CDD), prescribed in Article 5 of the Ordinance (suspicious transactions, and transactions conducted in significantly different mode from similar transactions)

○ Transactions with those who reside or are located in countries/regions considered to require attention, given the development status of their AML/CFT systems, in the NRA-FUR
○ Transactions that are deemed high ML/TF risks in light of the contents of the NRA-FUR

3. Assessment Methods

(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.

A. 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. For example, criminals, terrorist groups and their facilitators, their funds, ML/TF activities, etc.

○ Vulnerability

Things that can be exploited by the threat or that may support or facilitate the threat. For 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. For example, the impact on the reputation of a country's financial sector, etc.

B. 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

A. Assessment Method

Taking into account the FATF Guidance, this risk assessment uses a wide range of inputs including the information relating to ML cases and the measures being taken by AML/CFT stakeholders in accordance with the Act on Prevention of Transfer of Criminal Proceeds, as well as the FATF Recommendations and its Interpretive Notes[*1] and the findings pointed out in the Third Round Mutual Evaluation of Japan[*2]. In the analysis, the following factors are considered:

○ Threat

Example : Offenders including Boryokudan (Japanese organized crime groups), specialized fraud groups, and crime groups of foreigners in Japan[*1] , and predicate offences such as theft and fraud that generate criminal proceeds.

○ Vulnerability

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

○ Consequence

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[*2] in terms of products/services, transaction types, countries/regions, and customer attributes.

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, STRs, information concerning ML cases, and risk mitigation measures.:

B. Information Used in the Assessment

For the assessment, a wide range of sources of information were collected from domestic and international organizations, such as statistics and case analysis information. The information associated with products/services was also useful inputs provided by industry associations or business operators, with regard to the types, scales, etc. of the actual transactions, the level of awareness of business operators about ML/TF, and the status of their AML/CFT systems, etc.

In addition, investigated information on money laundering offences and STRs are used, which are mostly relating to case in the past three years.

4. Main Contents

(1) Main Assessment Findings from Preceding Years, etc.

The NRA-FURs have been published every year since 2015 and all reports are publicly available. NRA-FUR has broadened the scope of research and analysis in the process of preparation, as ML/TF risks surrounding Japan change. And it added descriptions about crypto assets, international terrorists, predicate offenses, etc. based on the results of research and analysis. Moreover, the assessment results of measures to mitigate the risks of products and services, including not only statutory measures but risk assessments and operational measures, such as the status of activities relating to risk-based approach performed by competent authorities and business operators, were also incorporated in the NRA-FUR.

The 2019 NRA-FUR added risks based on the trends of increasing foreign criminals and their countermeasures regarding ML/TF risks based on the status Furthermore, the description of fund transfer services, expected to increase in demand as the number of foreigners increases, was expanded. As in the past, the status of activities relating to risk-based approaches performed by the competent authorities and business operators is described. Besides, new survey results on matters identified by competent authorities for business operators to note are also added. For feeding back to business operators the fact that information on STRs reported by business operators is effectively used for investigating money laundering offenses and their premise offenses, information on STRs used for arrested cases was added.

As a future initiative based on the survey results, the NRA-FUR indicated to the competent authorities that it is necessary to deepen guidance and supervision including administrative guidance at the risk of the business type under its jurisdiction and business operators. The NRA-FUR also indicated to them the need to collaborate with

---

*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.

*2 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.

industry associations to raise the industry's level regarding AML/CFT measures and grasp the degree of establishment of efforts.

As a matter of course, the NRA-FUR shown necessary that business operators must not only thoroughly fulfill their legal obligations and formally confirm the existence of legal violations but identify the risks to be faced with comprehensively and concretely checking the characteristics of their own business and the risks associated with it., take substantial measures, and mitigate the risks.

(2) Main Assessment Findings from This Year, etc.

A. Overview of Findings

In the 2020 NRA-FUR, from the broader perspective of ML/TF risks across Japan, risk analysis on the environment surrounding Japan is newly added in the report. Furthermore, in response to the worldwide spread of the novel coronavirus infection, the criminal trends/typologies associated with the infections are analyzed in the same item (see *Section 2. Environment Surrounding Japan*). Furthermore, based on the current situation, the NRA-FUR expands the description of features and cases related to products and services, quasi-Boryokudan and international terrorists.

Besides, following the previous year's NRA-FUR, matters identified by competent authorities that business operators should note and business operator's activities, are described in Section4.Risk of Products and Services. The newly identified ones are listed at the end of this item.

Furthermore, for giving a feedback to business operators on the fact that information on STRs reported by business operators is effectively used for investigating money laundering offenses and their premise offenses the information on STRs used in arrested cases is expanded to include notifications from a wider variety of businesses and described at the end of *Section 3. Analysis of Money Laundering Cases, etc.* continuing from last year's NRA-FUR.

The NRA-FUR also describes measures to mitigate risks taken by the competent authorities in 2019 such as the publication or revision of guidelines to clarify the basic concept of effective ML/TF measures and the efforts to hold lectures on ML/TF measures in collaboration with other ministries and industry associations.

The NRA-FUR further describes the measures to mitigate risks taken by industry associations in 2019, including seminars on the Act on Prevention of Transfer of Criminal Proceeds, efforts to support AML/CFT measures such as providing document templates prepared by specified business operators and surveys on group member companies.

In 2019 there were measures to mitigate risks taken by business operators, such as activities that measures of risk-based approaches are taken against transactions evaluated as highly risky based on the risk index set independently by analyzing the business operators' business environment and the NRA-FUR described these.

The following describes matters for business operators to note, and examples of activities related to them as newly identified by competent authorities. Their details are described in *Section 4. Risk of Products and Services* of this NRA-FUR.

[Matters identified by competent authorities for business operators to note]

(Deposit-taking Institutions)

- ○ 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.
- ○ 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.
- ○ When opening an account of a foreigner, if the katakana name and alphabetic name is written on the customer identification documents, customer attribute of each name should be confirmed.
- ○ For transaction monitoring, it is necessary to set a scenario based on the own ML/TF risks, and consider other risks so that the monitoring targets are not biased toward specific financial crimes, such as specialized fraud cases.

○ Regarding transaction monitoring, it is necessary to set threshold values according to the customer risk assessments and regularly review scenarios and threshold values based on a financial crime pattern analysis.

○ For STRs, establish a system for appropriate examination and judgment, and utilize the status of STRs to strengthen an own risk control system.

(Insurance companies etc.)

○ 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.

○ Complying with domestic and foreign laws and regulations related to sanctions, taking other necessary measures, and building a framework to detect high-risk customers accurately.

(Financial instruments, business operators, etc.)

○ 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 the case of allowing high-value cash transactions at store counter, confirm and record the reasons for using such transactions and the payment route (whether the customers' funds, etc.), 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 due to the 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.

○ 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.

(Trust Companies etc.)

○ When analyzing risks, comprehensively and concretely analyze the risks, including analyzing STRs and reflecting them in document 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.

○ It is necessary to secure staff with expertise and suitability through recruitment and training in the sales department, management department, and audit department.

(Money Lenders, etc.)

○ In creating and reviewing documents prepared by specified business operators, they should quote the contents of national risk assessments and widely used templates. Not only that, but they should also consider the characteristics of their companies' transactions such as products, services, transaction forms, countries, and regions related to transactions, customer attributes, etc. and comprehensively 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.

(Fund Transfer Service Providers)

○ Establish an appropriate system to examine and manage agency and implement monitoring and training regularly and 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 preliminary examination on their association with antisocial forces, in addition to confirming that they are not spoofing, at the time of opening their account.

(Crypto-assets Exchange Service Providers)

- The management must formulate effective measures to mitigate risks and promote and establishing a system while taking the initiative and proactively participate in giving specific instructions and coordinating related departments.
- The management department must establish a system that can actively implement the risk-based approach and PDCA cycle and promote compliance with laws and regulations.
- Internal auditing is not limited to rule-based auditing but must conduct a risk-based approach.
- Measures to mitigate risks should not be limited to the application of legal requirements, such as verification at the time of transaction and to quoting the contents of national risk assessments and widely used templates. Regarding the results of an analysis to be compiled in a document prepared by a specified business operator, 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.

(Currency Exchange Operators)

- Appoint a manager (manager of verification at the time of transaction) responsible for the performance of verification at the time of transaction.
- 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.
- 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 STR(s).
- Appropriately recording reasons for determining that the transaction is not suspicious.

(Credit Card Operators)

- 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.

(Real Estate Brokers)

- 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.

(Dealers in Precious Metals and Stones)

- Strengthen education and training for employees and develop and review regulations to accurately perform verification at the time of transaction

(Postal Receiving Service Providers)

- Refer to the List of Reference Cases of Suspicious Transactions and consider the necessity for reporting STRs regarding transactions conducted by the company.

(Telephone Receiving Service Providers)

- Refer to the List of Reference Cases of Suspicious Transactions and consider the necessity for reporting STRs regarding transactions conducted by the company.

(Telephone Forwarding Service Providers)

- Refer to the List of Reference Cases of Suspicious Transactions and consider the necessity for reporting STRs regarding transactions conducted by the company.

(Legal/Accounting Professionals)

○ Lawyers

- 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.

○ Judicial scriveners

- Appropriately verify clients' identities by receiving the submission of identity verification documents.

○ Administrative scriveners

- Thoroughly verify the identity of the client.
- Appropriately create and save confirmation records.

○ Certified public accountants

- 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 evaluate 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.

○ Certified public tax accountants

- Conduct verification at the time of transaction, and appropriately create and save confirmation records.

[Examples of business operators' activities]

(Deposit-taking Institutions)

○ Cases where a transaction related to a business that handles products possibly used for military purposes is specified explicitly as a high-risk transaction with consideration of information published by competent authorities.

○ Cases where a customer reported with STRs in the past is evaluated as high-risk customer according to the content of the notification.

○ Cases of correspondent management where risk is evaluated by focusing on the correspondent's business area, attributes, business content, and the presence or absence of disposal related to ML/TF.

○ Cases of a customer who was reported with STRs in the past, where an information-sharing system is established and when dealing with the customer, details are confirmed by checking the documents and interviewing and then transaction is approved by the senior manager.

○ Cases where 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 a category, 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 the senior administrator's confirmation.

○ Cases where a business operator's environment, strategy, geographical characteristics in the sales area, and its customers' characteristics are analyzed to extract unique risk indicators from the geographical characteristics of business areas, such as being close to airports and ports. The business operator identifies vendors that may dismantle, purchase, 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.

○ Cases of non-face-to-face transactions, where transaction monitoring is conducted focusing on access information, such as IP addresses and browser languages, with consideration of the possibility of spoofing.

(Financial Instruments Business Operators, etc. and Commodity Derivatives Business Operators)

○ The confirmation and management of foreign customers' period of stay, the confirmation of the beneficial owners of legal persons using a third-party information agency, and freezing and transaction suspension of non-operating accounts as an example of enhanced customer due diligence.

○ An example of transaction monitoring is promoted by adding deposit and withdrawal monitoring scenarios and grasping overseas transactions by detecting IP addresses.

○ An example of promoting cooperation, such as sharing necessary information and strengthening the reporting system as an initiative between the same financial group companies.

(Trust Companies etc.)

○ Cases where risk assessment is performed for each customer considering the products, services, transaction types, countries, regions, and customer attributes and measures are taken according to the assessment.

○ Cases of continuous checks on business partners' relationship with antisocial forces and records on economic sanctions, where business operators implement customer due diligence according to the trustors and trustees' risks, considering that valid right holders and their objects may become opaque due to the trust relationship.

(Money Lenders, etc.)

○ Cases of checking phone numbers noticed by customers with a business operator's database to ascertain that the customers' telephone numbers are unique.

○ Cases of detecting suspicious and unnatural transactions by utilizing IT vendors' systems and grasping when the telephone numbers notified by the customers were used.

(Fund Transfer Service Providers)

○ Cases of identifying and evaluating risks for services provided by a business operator acting as issuers of cards using the pre-paid payment methods when fund transfer services operate an issuer of that as a side job.

(Crypto-assets Exchange Service Providers)

○ Cases where as of the risk of using services in process of specialized fraud, the results of investigation and analysis related to the unnatural matching of customers' characteristics, such as their photos on identity verification documents and customer attributes found in the verification at the time of transactions, are reflected in documents prepared by specified business operators and verification at the time of transactions is strengthened.

○ Cases of strengthening the monitoring of transactions with countries judged to be highly risky and customers in the same countries by focusing on prosecution cases and media reports on financial crime-related remittances, risk analyses and the corruption perception indexes (CPIs) conducted by other countries' authorities.

○ Cases where the period of stay of foreign customers, such as international students and workers, is managed by a system after confirming it to deal with risks such as the sale of accounts at the time of their return to their home countries.

(Currency Exchange Operators)

○ Cases where 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.

○ Cases where 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.

(Legal/Accounting Professionals)

○ Lawyers

- Cases where a lawyer did not accept a Japanese enterprise's request, due to a high risk of money laundering when the enterprise without introduction inquired about payment via the law firm when sending money to a foreign company, since the business content of the Japanese company was not familiar to the law firm.
- Cases where risks are identified, evaluated, and mitigated, in the acceptance decision after inquiring the counterpart of the client's business or proposed project whether there is property to be transferred and whether the proposed transaction is standard with consideration of the client's business type. At the first interview, the lawyer confirms any financial difficulties or unusual points. In addition to independent and reliable public information sources, such as corporate registration, the lawyer uses public Internet information sources and inquiries.
- Cases of using domestic and foreign databases and investigating whether clients are antisocial forces or foreign PEPs in the decision to accept requests from clients.
- Cases of building an internal control system by creating and disseminating internal regulations and manuals related to ML/TF measures, training and briefing sessions for lawyers and staff, and establishing responsible departments, such as internal control committees in the law office.
- Cases of promoting clients' cooperation and confirming appropriately customer identity, where delegation contract and advisory contract templates stipulate that the law firm can request principle identification documents. The clients should notify if there is a change in customer identity.

○ Certified public accountant or audit firm

- Cases of concluding new contracts, where the risks are classified according to the contract destinations' business types, and the higher the risk, the more materials are used to examine the contracts.
- Cases of continuing audit contracts (renewed initially every year), where the types of industries, officers, significant shareholders, etc. are confirmed.
- Cases of conducting new contracts for specific industries where there are in-depth investigations based on past data.

B. Measures Related to the Act on Prevention of Transfer of Criminal Proceeds

The Act on Prevention of Transfer of Criminal Proceeds provides that insofar as necessary to enforce the Act, competent authorities shall request reports or documents from specified business operators, conduct on-site inspections, provide guidance, issue rectification orders, etc. and the National Public Safety Commission shall provide statements of opinion to the competent authorities and conduct inquires necessary for this purpose. It furthermore stipulates penalties for violations of rectification orders.

The reports for specified business operators collected by the National Public Safety Commission in 2019(see table 1) were all for telephone forwarding service providers, and specific violations found by this was recognized as follows:

- ○ Neglected to verify the purpose of customers' transactions, their occupations, etc.
- ○ Lacking confirmation of customer identities with valid identity verification documents.
- ○ Neglected to send transaction-related documents by registered mail that must not be forwarded or the like in non-face-to-face transactions.

Considering the results of the collection of reports, the National Public Safety Commission stated that competent authorities with jurisdiction over telephone forwarding service providers should take necessary measures to correct specified business operator's violation of the Act on Prevention of Transfer of Criminal Proceeds.

Between 2017 and 2019, three rectification orders were issued under the Act (see table 1), mainly concerning offenses related to verification at the time of transaction and the preparation and keeping of verification records. Regarding these offenses, competent authorities ordered specified business operators to take the following rectification measures within fixed periods of time:

- ○ Reaffirm provisions of the Act on Prevention of Transfer of Criminal Proceeds through in-house education, etc.
- ○ Develop manuals to smoothly perform procedure regarding the Act on Prevention of Transfer of Criminal Proceeds
- ○ Develop recurrence prevention measures, and review practices
- ○ Perform verification at the time of transaction concerning customers who had signed contracts in the past, and prepare and keep verification records

Table 1 [Numbers of Reports Collected by the National Public Safety Commission/National Police Agency and of Rectification Orders Issued by Competent authorities Receiving Statements of Opinion (2017–2019)]

Year / Category	2017	2018	2019
Number of reports collected by the National Public Safety Commission	7	13	7
Number of directions for prefectural police to conduct inquiries	0	0	0
Number of opinion statements made to competent authorities	7	11	8
Number of rectification orders based on opinion statements	1	1	1

C. Future Activities

In light of the result of this year's NRA-FUR, competent authorities must continue to ensure that business operators thoroughly fulfill their legal obligations. At the same time, they will need to expand guidance/supervision, etc. commensurate with the risks, associated with business categories or business operators under their jurisdiction. Furthermore, it is necessary for them not only to provide appropriate guidance/supervision, including administrative guidance, to business operators who fall short in proactively engaging in such activities, but also to share information necessary for the activities, countermeasure cases, including STRs and system development, etc. with such business operators, in collaboration with industry

associations, etc. and then they continuously need to grasp the level at which the activities have been established, in order to raise the level of AML/CFT systems across the entire industry.

It goes without saying that business operators need to thoroughly fulfill their legal obligations, but they also need to go beyond verifying whether they have committed any violations of laws, regulations, etc. as a matter of formality while being aware of STRs. They will continuously need to make comprehensive and specific assumptions about their business characteristics and the risks involved, identify the risks they face, and take measures substantially. Especially for products/services whose risks of misuse for money laundering are considered to be relatively higher than those of other business categories or be increasing, it is necessary to put appropriate and substantial AML/CFT measures in place according to respective risks, and take measures to mitigate risks.

In addition, competent authorities have been continuing to promote publicity activities for the public through various means and methods. This is because it is crucial for the public to raise awareness of AML/CFT measures through collaboration between administrative authorities and business operators, etc., understand the importance of the measures, and gain their cooperation in taking AML/CFT measures taken by business operators, etc. Essentially, this means getting the whole country to promote AML/CFT measures.

Section 2. Environment surrounding Japan

This NRA-FUR identifies high risk transactions from the viewpoints of products and services, transaction types, countries and regions, and customer attributes, which are based on cross-sectional analyzing money laundering cases, etc. (offenders, modus operandi) and risk of products and services, given various ML/TF risks surrounding Japan. And the above is described in and after *Section 3. Risk of Products and Services*. Multifaceted and comprehensive risk assessment is conducted based on the situation regarding the measures taken to mitigate the identified risk.

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 population estimate (Statistics Bureau, Ministry of Internal Affairs and Communications), Japan's total population as of October 1, 2019, was 126,167,000, a decrease of 1.5% compared with the statistics ten years ago (2010).On the other hand, the aging rate as of October 1, 2019 (the ratio of the population aged 65 and over to the total population) reached a record high of 28.4%, an increase of 5.4 points compared to the aging rate of 23.0% 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, specified industrial fields have difficulty securing human resources to respond to the severe labor shortage. In that field, it is necessary to build a mechanism to accept foreigners who have a certain level of expertise and skills and are ready to work. Therefore, the statuses of residence as 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 page 19 Status of Entry/Residence of Foreigners in Japan).

3. Economic Environment

Japan's economic situation 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 2019 was 553.7 trillion yen, the third-largest economy after the United States and China. In terms of purchasing power parity GDP, it is the fourth largest globally after China, the United States, and India. The real GDP growth rate in FY2019 was 0.0%. The share of the composition ratio (nominal) of GDP by economic activity in 2018 was 1.2% for the primary industry, 26.6% for the secondary industry, and 72.2% for the tertiary industry. Regarding the trade value in 2019, Japan's exports amounted to 76,931.7 billion yen, and imports amounted to 78,599.5 billion yen. The main export partners were the United States, China, and South Korea, and the import partners were China, the United States, and Australia. 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.

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 2019, the number of branch offices of major financial institutions[*2] was 37,627 (including 174 overseas branch offices). There were 98,442 ATMs installed with ease of access to the financial system. Furthermore, three of the 30 global

---

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

systemically important banks (G-SIBs) designated by the Financial Stability Board (FSB) in 2019 were Japanese megabanks, and 25 G-SIBs have branch offices, etc. in operation in Japan.

In terms of the scale of financial transactions in Japan, the balance of bank deposits at the end of September of 2019 was approximately 818 trillion yen. As for settlement transactions, the handling status of domestic exchange (other banks' transaction volume of exchange) in 2019 was approximately 2,897 trillion yen (approximately 1.7 billion cases), and the daily average was about 12 trillion yen (approximately 6.88 million cases). The amount of foreign exchange in yen settlement during the same year was approximately 4,308 trillion yen (approximately 7.28 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 672 trillion yen as of December of 2019. In terms of market capitalization classified by country, Japan ranks third after the United States and China. It 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 2019 was approximately 604 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 deposit money into accounts. Furthermore, there is "adequate security" with few thefts and the cases that lost money 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, with the cashless payment ratio rise due to progress of cashless payments, cash transaction has decreased relatively. 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 4. 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 situation, 748,559 of recognized criminal offenses cases were recognized in 2019. This number renewed the lowest after the Second World War recorded continuing from the previous year. The rate of decrease from 2002, when the number of recognized criminal offenses cases was the highest after the Second World War, was 82.8% (the total number of cleared criminal offenses was 294,206, and although it continued to decline, the rate of arrests was 39.3%, up 1.4 points from the previous year). The number of elderly victims to the number of recognized criminal offenses has consistently increased since 2009. In 2019, it was 12.3%, up 3.8 points from 8.5% in 2009. 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 33.9% in 2019, an increase of 25.0 points from 20 years ago. Furthermore, in terms of the situation of damage to the elderly with the specialized fraud group, which is the main offenders of money laundering in Japan (see *Section 3. Analysis of Money Laundering Cases*), the ratio of damage to elderly to the total number of cases of specialized fraud was 83.7% in 2019. Given the aging population, in which the population of people aged 65 and over increases while the total population is declining, it is necessary to continue paying close attention to specialized fraud and take measures.

The number of cleared money laundering cases in Japan is on the rise, and the number of cleared cases in 2019 (537 cases) reached a record high. In terms of the cleared cases, Boryokudan members, associates and other related parties and crime groups of foreigners in Japan are skillfully conducting money laundering (see *Section 3. Analysis of Money Laundering Cases*).

Next, looking at indicators other than the number of recognized criminal offenses, the number of cleared cybercrimes is rising. The number of those cleared cases (9,519) in 2019 was the highest ever. From 2016 to 2018, the number of cases and the amount of financial damage over illegal remittance offences related to Internet banking continued to decrease due to the strengthening of financial institutions' security measures. However, the number of victims increased sharply from September of 2019. Both the number of cases and the amount of financial damage increased significantly compared to the previous year. Most of the damage is believed to be due to phishing disguised as a financial institution. The number of accesses considered to be search activities in cyberspace detected by the National Police Agency is also rising.

(2) Terrorism Situation

As for international terrorist situation, ISIL[*1] calls on sympathizers to carry out terrorism against Western countries participating in the willing anti-ISIL coalition. Besides, AQ[*2] and related organizations are also calling to execute terrorism against the United States and other countries. Furthermore, terrorist attacks have occurred one after another in various parts of the world. There have also been cases in which Japanese people's interests and related Japanese facilities have been damaged overseas by terrorism. It can be said that the threat of terrorism against Japan continues. It has been a long time since the alleged abduction by North Korea occurred. However, all victims' return has not yet been realized, and the situation is such that a momentary grace is not 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.

[Crime status related to the novel coronavirus infection]

1. Criminal status related to novel coronavirus infection

(1) Situation

As the novel coronavirus infection spreads worldwide, it is expected that fraud and cybercrime related to the infection will increase and that the form of crimes of various illegal fundraising activities will change. Therefore, there is concern that ML/TF threats will increase along with this. International organizations, such as the International Criminal Police Organization (INTERPOL), are calling attention that fraud and cybercrime methods that have taken advantage of the spread of the novel coronavirus infection. In Japan, the National Police Agency and the Consumer Affairs Agency are also calling attention to suspicious phone calls and e-mails that have taken advantage of the spread of the novel coronavirus infection.

(2) Situation of Crime Occurrences in Japan

Also, in Japan, the following cases related to the novel coronavirus infection have occurred. It is expected that threats, of ML/TF associated with the novel coronavirus infection, will continue to increase in the future.

- ○ A case of trying to cheat cash in the name of inspection fees for the novel coronavirus infection.
- ○ A case where a deceived victim transferred cash to a designated account in the name of a loan deposit for the novel coronavirus infection.
- ○ A case where an offender pretended to be a city hall official and finagled a cash card in the name of a benefit payment procedure.
- ○ The offender, who pretended to be an employee of a foreign company with a business relationship, send an e-mail with content that the financial institution for regular transactions could not be used because of the novel coronavirus infection's influence and the price of product should be transferred to the account of another financial institution. Then it was transferred and finagled.
- ○ A case where Boryokudan gangster, etc. applied for a loan related to the novel coronavirus infection to a financial institution and tried to deceive the loan even though they were not business operators.
- ○ A case where a Brazilian who ran a restaurant and a Japanese offender colluded to apply for a leave request support fund to be paid in response to a leave request and they tried to receive it to a financial institution's account. However, the restaurant was not cooperating with the request for leave for measures against the novel coronavirus infection.
- ○ A case of stealing money and things at a restaurant that was closed in connection with the novel coronavirus infection.
- ○ A case where a person not registered in the money lending business purchased wage receivables from those who needed living due to the effects of the novel coronavirus infection and in exchange for those delivered money as the debt after deducting unlawful fees. After that, a person collected the debt.

---

*1 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.

*2 Abbreviation for Al-Qaeda

- A case of a loan shark lending at a high-interest rate to those whose income decreased due to the influence of the novel coronavirus infection.
- A case of reselling sanitary masks and alcohol for disinfection at a price exceeding the purchase price.

(3) Analysis of STRs

Analysis on STRs thought to have been affected by the novel coronavirus infection indicated the main ones described below. We want the business operators to deepen their awareness of ML/TF risks affected by the novel coronavirus infection and their measures taken by their risk-based approach, by referring to the following contents.

- As there was a suspicion of spoofing transaction, the customer was asked to confirm the personal identification items in person. However, the customer refused because of concerns about infection with the novel coronavirus infection.
- When a customer was depositing a large amount of cash into the customer's account with a financial institution, the source of funds was unclear due to ambiguous reasons, such as avoiding financial risks related to the novel coronavirus infection.
- The project scale and transaction details were not consistent with the amounts of remittances as assistance for people who have financial difficulties in living due to the effects of the novel coronavirus infection or export prices of virus protective clothing.
- There was a case of allocating borrowings from a local financial institution for measures against the novel coronavirus infection to fund of foreign remittances to purchase foreign real estate. Borrowing is used for purposes other than the original purpose of borrowing.
- A customer who applied to open an account with a financial institution to receive benefits related to the novel coronavirus infection turned out to be a member of antisocial forces, such as Boryokudan gangster.
- A customer who applied to open an account with a financial institution to receive loans related to the novel coronavirus infection was found to be a dormant corporation or a legal person without transparency.
- There were cases suspected of being damaged by specialized fraud, business email fraud, and investment fraud that took advantage of the spread of the novel coronavirus infection.

2. Impact on Competent authorities and Business Operators

The spread of the novel coronavirus infection is expected to affect the emergence of new ML/TF risks and the competent authorities and business operators' responses to money laundering. FATF issued COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses (May 2020), which describes threats and vulnerabilities of ML/TF resulting from the spread of the novel coronavirus infection. There is concern that ML/TF risks will increase in Japan due to an increase or decrease in transaction volume due to changes in household spending and transaction form changes, such as shifting from face-to-face transactions to non-face-to-face transactions to prevent infection. Furthermore, there will be an increase in customers' requests different from those in normal times due to unstable social and economic conditions. There are some business types in which the transaction volume has changed due to a decrease in foreign visitors to Japan and Japanese overseas travelers. This change is due to the reinforcement of border countermeasures against the novel coronavirus infection. Business operators are required to take an even more effective risk-based approach to respond flexibly to the ever-changing economic and social environment.

Competent authorities should review the measures to mitigate ML/TF risks by considering transaction monitoring and threshold changes and proactively work on supervision and guidance by a risk-based approach according to changes in the transaction type of the business types under their jurisdiction.

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 in 2019, 58 cases (10.8%) were related to Boryokudan members, associates and other related parties (hereinafter referred to as "Boryokudan gangsters") (see Table 2). Out of those, 51 cases fell under the Act on Punishment of Organized Crimes, Control of Crime Proceeds and Other Matters (32 for concealment of criminal proceeds and 19 for receipt of criminal proceeds) and seven fell under the Anti-Drug Special Provisions Law (six for concealment of illegal drug proceeds and one for receipt of illegal drug proceeds).

In addition, considering the involvement of Boryokudan gangsters in relation to predicate crimes of money laundering crimes in the last three years, the majority of cleared cases have been for fraud and theft. On the other hand, when looking at the number of Boryokudan gangsters as a proportion of arrested offenders, it appears that their ratio in gambling, blackmailing, illicit drugs, and prostitution offenses is high.

Boryokudan repeatedly commit crimes professionally to gain economic profit, and are skilled at money laundering.

Money laundering by Boryokudan seems to be carried out internationally, In the U.S. "Strategy to Combat Transnational Organized Crime" was published and a Presidential executive order 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 in *Section 5 High-risk Transactions 3. Customer Attributes and Risks (1) Anti-social Forces (boryokudan, etc.)* also explains the survey results and analyzes them.

Table 2 [Number of Cleared Money laundering Cases (Committed by Boryokudan Gangsters) under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law (2017–2019)]

Category \ Year	2017	2018	2019
Cleared cases of money laundering offenses	361	511	537
Cases by Boryokudan gangsters	50	65	58
Percent (%)	13.9%	12.7%	10.8%

(2) Specialized Fraud Group

Japan has recently witnessed a rise in specialized fraud cases[*1] (see table 3). Damage in 2019 was concentrated in metropolitan areas. Tokyo (3,815 cases) accounted for 22.6% of the total number of cases recognized, and five prefectures, including Kanagawa (2,793 cases), Saitama (1,459 cases), Chiba (1,409 cases), and Osaka (1,809 cases), accounted for 67.0% 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 other parties as a means to receive money from a victim. Furthermore, crime bases have spread to rental condominiums, rental offices, hotels, vehicles, etc., and the existence of foreign crime bases has surfaced.

---

*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.

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 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 3 [Number of Recognized Specialized Fraud Cases and Total Financial Damage (2017–2019)]

Category \ Year	2017	2018	2019
Number of recognized cases	18,212	17,844	16,851
Total financial damage (yen) (Effective total amount of financial damage)	39,474,870,491	38,286,761,222	31,582,937,585

Note 1: Data from the National Police Agency

2: Since 2018, cases have been increasing where the criminal in the role of receiving the cash card meets the victim who has already been deceived by phone and secretly swaps the cash card with another card by seizing an opportunity. 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).

(3) Crime groups of foreigners in Japan

Criminal proceeds from offenses in which foreigners are involved are difficult to be traced because they are transferred across borders between countries of different legal and transaction systems. Such crimes have characteristics that their human networks, manner of offenses, etc. are not limited within one country as seen in cases where crime groups consisting of foreigners in Japan, etc. commit crimes following instructions from criminal groups existing in their home countries, and these offenses tend to be more sophisticated and hidden as the roles of offenders are divided across borders.

Of cleared money laundering cases in 2019, 71 cases (13.2%) were committed by foreigners in Japan (see table 4). The breakdown comprised 49 cases of concealment of criminal proceeds and 22 cases of receipt of criminal proceeds.

Table 4 [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 (2017–2019)]

Category \ Year	2017	2018	2019
Cleared cases of money laundering offenses	361	511	537
Cases by foreigners	27	48	71
Percent (%)	7.5%	9.4%	13.2%

In the cleared money laundering cases 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 the total.

*1 China in this survey does not include Taiwan or Hong Kong unless otherwise specified.

Observations of the situation indicate that money laundering offenses are committed in organized-crime operations by foreigners in Japan, and there were money laundering offenses associated with cases of illegal remittance offenses pertaining to Internet banking systems by a group of Chinese, shop lifting offenses by a group of Vietnamese, and international fraud offenses by a group of Nigerians.

In addition, by nationality Vietnam and China lead the rankings of numbers of cleared offenses and account for more than 80% of the total 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.

Furthermore, with respect to the number of STRs in the last three years, STRs related to China, Vietnam, and Korea are the top 3 by number, and recently there has been a remarkable increase in reports related to Vietnam.

With respect to international transactions, this NRA-FUR in *Section 5 High-risk Transactions 1. Transaction Type (3) International Transactions* also explains the results of surveys and analysis.

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

[Status of Entry/Residence of Foreigners in Japan]

The number of foreigners entering Japan in 2019 was 31,187,179. Of these, the total number of new arrivals was 28,402,509 and 4.6 times as many compared to that of 10 years before (2009). In terms of the number of new arrivals by nationality and region, the Chinese accounted for about 30% of the total, followed by South Koreans, Taiwanese, Chinese (Hong Kong), and Americans. Looking at this by purpose (status of residence), the number of Temporary Visitors was the largest (27,810,548), accounting for 97.9% of the total number of new arrivals, followed by foreigners with the status of residence as Technical Intern Training No. 1 (173,705), those with the status of Residence as Student (121,637), and those with the status of Residence as Entertainment (45,486), accounting for 0.6%, 0.4%, and 0.2%, respectively. The number of new arrivals (173,705) with the status of residence as Technical Intern Training No. 1 has shown a high increase, of up 20.5% from the previous year. In terms of the new arrivals of those with the status of residence as Technical Intern Training No. 1 by nationality and region, the number of Vietnam was 91,170, accounting for 52.5% of the total, followed by Chinese (20.0%), Indonesians (9.1%), Filipinos (8.0%), and Myanmarese (3.7%).

Next, in terms of the number of foreign residents, the number of mid-to-long-term residents in Japan as of the end of 2019 was 2,620,636, and the number of special permanent residents was 312,501. The total number of foreign residents was 2,933,137, an increase of 202,044 (7.4%) from the end of the previous year. It was an increase of more than 30% from 10 years before. The ratio of foreign residents to Japan's total population at the end of 2019 was 2.32%of the total population of 126.17 million (as of October 1, 2019, Population Estimate (Statistics Bureau, Ministry of Internal Affairs and Communications)), 0.16 points higher than 2.16% at the end of the previous year and 0.66 points higher than ten years before. In terms of the number of foreign residents by nationality and region as of the end of 2019, Chinese accounted for 27.7% of the total (813,675 residents), followed by South Koreans 15.2%, Vietnamese 14.0%, Filipinos 9.6%, and Brazilian 7.2%.

[Recent situation surrounding crimes committed by foreigners in Japan]

The number of cleared cases involving foreigners in Japan indicates that the number has remained relatively stable in recent years. In terms of the total number of cleared cases and offenders by nationality, Vietnamese and Chinese account for more than 50% of the total. In terms of the total number of cleared cases, in 2010, Chinese accounted for 36.5% of the total. However, in 2019, the ratio dropped to 26.0% while that of Vietnamese surged from 8.9% to 35.0%. The total number of cleared Vietnamese case was the highest in 2019, overtaking that of Chinese. The breakdown of total offenders in cleared cases by visa status indicates that those who are Temporary Visitors, Students, and Technical Intern Trainees were high. Among them, an increase in Technical Intern Trainees is remarkable. The rate of complicity cases involving foreigners among the number of cleared criminal offenses is about 3.1 times that of Japanese, suggesting that crimes committed by foreigners in Japan tend to be carried out in an organized manner. The total financial damage from property offenses committed by foreigners in Japan among cleared cases in 2019 was about 2 billion yen, of which theft accounted for about 1.1 billion yen (55.1%), and fraud accounted for about 880 million yen (44.2%). The number of cleared cases of criminal offenses by crime type indicates that theft is highest for Vietnamese and fraud is highest for Chinese in terms of nationality. In terms of cleared cases for crime infrastructure related offenses, forgery of passports, residence cards, etc., are used to disguise residence status that allows work. It has been on an increasing trend since 2016.

In recent years, most Vietnamese crimes have been theft, and shoplifting is high on a method-by-method basis. As a form of shoplifting crime, after receiving instructions from a ringleader in their own country via a social networking service (SNS) site, a group of several people shares the role of a watchman, actor, and product unloader, etc. They ride in a vehicle to a large drug store, supermarket, etc., shoplift large amounts of products, such as Japanese cosmetics, popular mainly in Vietnam, and export them overseas. Their organizational scheme

and planning are recognized. Furthermore, in terms of the number of people cleared for underground bank offenses by nationality, Vietnamese has the largest number.

Recent crimes committed by Chinese include obtaining a large quantity of products under false pretenses by using elaborately forged credit cards or illegally obtained information on mobile electronic payment systems belonging to other persons. In addition, there have been comparatively more cleared cases of crime infrastructure related offenses including bogus marriages, forged passports/resident cards involving Chinese than those cases committed by foreigners from other countries. Chinese offenders often use smartphone apps, etc. as a means of communication, which increases the anonymity and widespreadness of crime.

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

1. The following are money laundering offenses involving Vietnamese:
   - ○ Case of operating an underground bank by accepting overseas remittances using an SNS and transferring cash to accounts of another party opened in Japan.
   - ○ Case where the sales proceeds of forged residence cards were transferred to accounts to conceal criminal proceeds.
2. The following are cases involving Chinese in money laundering offenses:
   - ○ Case where an offender concealed the criminal proceeds obtained through unauthorized access to Internet banking by transferring them to multiple illegally obtained accounts under the name of Vietnamese persons
   - ○ Case where an offender concealed the criminal proceeds obtained through illegal reselling of pharmaceuticals by transferring them to an account under the name of an acquaintance of the offender
   - ○ Case where an offender concealed the sales proceeds of forged brand goods by transferring them to illegally obtained accounts under the name of a Japanese person
   - ○ Case of using forged credit cards or fraudulently obtained credit card information to impersonate the cardholders to obtain cigarettes, cosmetics, etc. by pretenses.
3. The following are examples of cases involving other foreigners in Japan in money laundering offenses:
   - ○ Case where Nigerians and others concealed criminal proceeds by deceiving an American company into transferring money to an account opened in Japan under the name of a legal person, by sending bogus e-mail, etc.
   - ○ Case where Nigerians and others concealed criminal proceeds by deceiving a woman with whom they became acquainted through SNS into remitting money from defrauded to an account opened in Japan under the name of another party
   - ○ Case where a Malaysian was given instructions from another offender via SNS to receive forged credit cards stored in coin-operated lockers

2. Modus Operandi

(1) Predicate Offenses

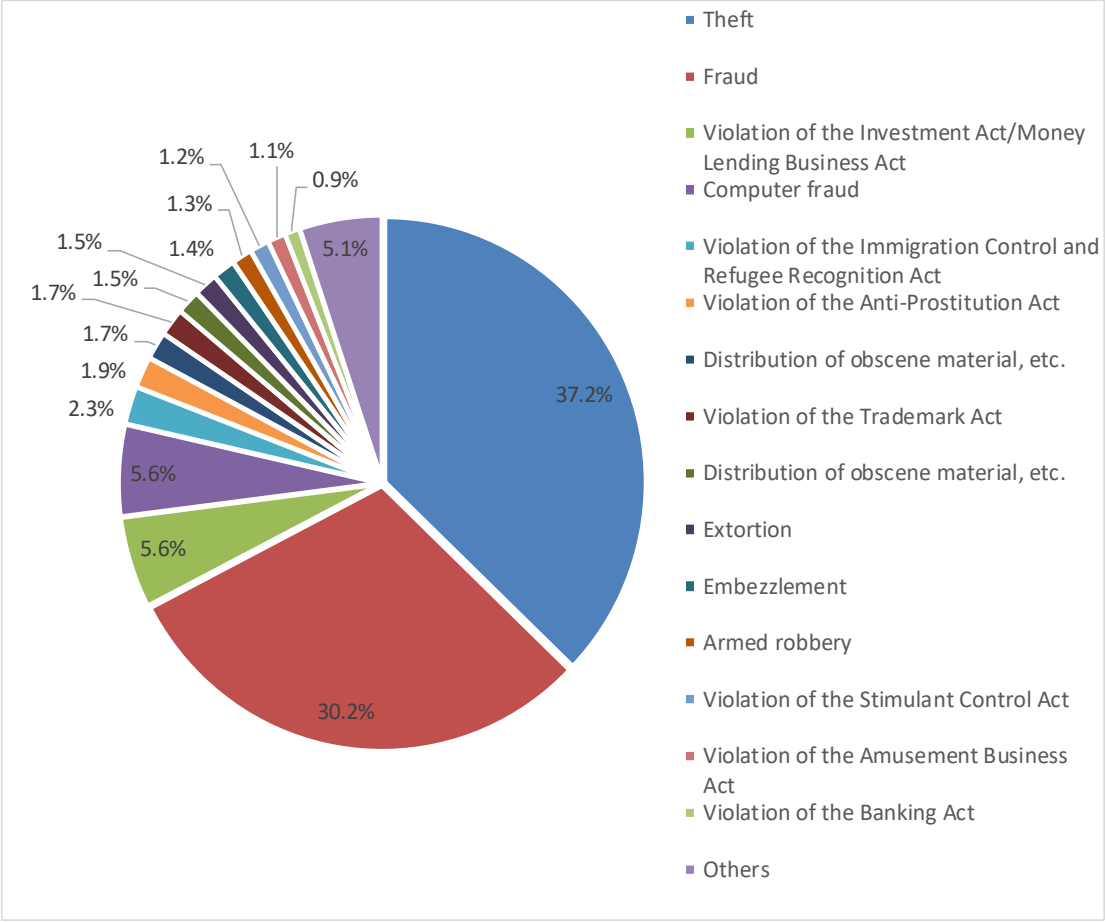
Money laundering offenses prescribed in the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Law are concealment and receipt of proceeds from specific predicate offences and certain actions to control the business operations of companies by using such proceeds. In June 2017, the Act on Punishment of Organized Crimes was revised to substantially increase the types of predicate offenses. They include offences 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 offences, as well as offences subject to the Immigration Control and Refugee Recognition Act (Cabinet Order No. 319 of 1951), 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 2017–2019[*1], theft was the leading crime with 533 cases, accounting for 37.2%, followed by fraud (432 cases for 30.2%), violation of the Investment

*1 There were 1,409 cleared cases of money laundering under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law from 2017 to 2019. On the other hand, the total number of cleared money laundering cases counted by predicate offenses was 1,432 (See Table 5) because some money laundering cases can be counted in multiple predicate offenses.

Act/Money Lending Business Act (Act No. 32 of 1983) (80 cases for 5.6%), computer fraud (80 cases for 5.6%), and violation of the Immigration Control and Refugee Recognition Act (33 cases for 2.3%) (see Table 5).

Table 5 [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 (2017–2019)]



Predicate Offenses	Theft	Fraud	Violation of the Investment Act/Money Lending Business Act	Computer fraud	Violation of the Immigration Control and Refugee Recognition Act	Violation of the Anti-Prostitution Act	Distribution of obscene material, etc.	Violation of the Trademark Act	Distribution of obscene material, etc.	Extortion	Embezzlement	Armed robbery	Violation of the Stimulant Control Act	Violation of the Amusement Business Act	Violation of the Banking Act	Others	Total
Total	533	432	80	80	33	27	24	24	21	21	20	18	17	16	13	73	1432
Ratio (%)	37.2	30.2	5.6	5.6	2.3	1.9	1.7	1.7	1.5	1.5	1.4	1.3	1.2	1.1	0.9	5.1	100

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. Major predicate offences are analyzed below.

A. Theft

(a) Forms of offenses

The forms of theft offences are diverse. Generally, there are cases where the amount of financial damage is comparatively small, but there are also cases committed professionally and repeatedly by crime organizations such as 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 drawn 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 2019 was about 63.3 billion yen (about 19.1 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 offences related to theft as predicate offenses, other than cases of buying and keeping stolen cars knowing that they are stolen, the following cases also occurred: a large number of coins obtained via burglary were deposited into and drawn from an account of another party, resulting in factual exchange; a large quantity of stolen gold ingots was sold to a gold trader in the name of a corporation operated by a friend of the offender; 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 other than actual residences as the destinations; and 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 professionally and systematically committed by domestic and foreign criminal groups. Large amounts of criminal proceeds are generated through economic activities disguised as legitimate operations, such as using bank accounts in the name of fictitious persons or other parties and through transactions by a corporation 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, 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.

The total financial damages from fraud offenses in 2019 was about 46.9 billion yen (cash damage total about 42.6 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 1.46 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 1.967 million yen per case.

(b) Modus operandi of money laundering

Regarding the modus operandi of money laundering offenses related to fraud as predicate offenses, in many cases damages from specialized fraud offenses are transferred to bank accounts in the name of fictitious or other parties. Also, 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 avoid financial institutions or the like freezing accounts once they have detected the damages. Holders of accounts used for concealment differ depending on the form of the offence; they may be individual persons, corporate bodies, or individual persons accompanied by a business name. There are actual cases where a foreigner in Japan had sold his bank account when leaving

Japan and the account was used to receive proceeds of specialized fraud offenses; a dummy corporation was established to open deposit accounts for receiving proceeds of specialized fraud offences; and an account in the name of an individual person accompanied by a business name was opened to receive proceeds from fraud offenses committed in a foreign country.

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

Computer fraud is applied to specialized fraud and Internet banking fraud, etc.

Cash cards obtained through deceiving victims and cash cards stolen account for more than half of all specialized fraud types. Criminals operate ATMs using cash cards that have been obtained through cheating victims, illegally transfer money from the victims' accounts to other accounts managed by the criminals.

In terms of illegal remittance offenses related to Internet banking, there were cases where illegal remittances were made from other parties' accounts to other accounts managed by the criminals by illegally accessing the business system managed by financial institutions using IDs, passwords, etc. of other parties. The financial damage in 2019 consisted of 1,872 cases, and the amount was approximately 2.521 billion yen. The number of cases in 2019 was the second highest after 2014. In 2014, the number of cases hit the highest ever. The amount of financial damage in 2019 increased significantly compared to the previous year. Most of the damage was considered to have used short message service (SMS) or e-mail methods to lead victims to phishing sites disguised as financial institutions. It has been confirmed that a phishing site stole the victim's ID, password, one-time password, etc., and the criminal illegally remitted money on the website of a financial institution. Furthermore, it has also been confirmed that the victim's ID and password, and information, including the victim's date of birth and telephone number, were stolen to make an illegal remittance using the official app of a financial institution. Of the 2,399 bank accounts identified as the primary destinations for illegal remittances, Japanese accounted for about 58.6% of the nationalities of the account holders, followed by Vietnamese (about 13.5%) and Chinese (about 8.8%).

As explained above, while Boryokudan involvement is observed in specialized fraud offenses, international criminal organizations have also been observed engaging in illegal remittance offenses related to Internet banking. 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

As for the modus operandi of money laundering offences related to computer fraud as predicate offenses, there were cases where 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 managed by the criminals from the accounts of the victims. Also, a criminal organization in China illegally accessed the business system of a financial institution in Japan and illegally remitted money to an account in the name of another person, and a criminal group of Chinese in Japan withdrew cash from the account. Furthermore, there were cases where 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 a form of loan-shark crime whereby a money lending business operates without a registration and lends 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 in the name of another party. Lenders may send direct mail based on lists of heavy debtors or solicit an unspecified large number of persons through internet advertisements or phone calls.

Large amounts of criminal proceeds are generated, and in 2019, the amount of damages reached over 6.7 billion yen, according to the statistics on cleared loan-shark crimes. In addition, it is recognized that Boryokudan professionally and continuously conduct loan sharking as an important source of revenue.

(b) Modus operandi of money laundering

Regarding modus operandi of money laundering offences related to loan-shark crimes as predicate offenses, there have been cases where debt repayments were remitted to accounts in the name of another party to conceal debt repayments to the loan-shark offenders. These accounts were obtained by the loan-shark offenders as debt repayments from borrowers and illegally used to conceal criminal proceeds.

In addition, there have been cases where loan-shark offenders required borrowers to send repayments to a post-office box opened in another individual's name or in the name of a fictitious business operator. In other cases, loan-shark offenders had made borrowers issue bills and/or checks when borrowing, and if there was any delay in repayment, collection would be made by a financial institution and payment is made to an account in 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 with a credit card.

E. Habitual gambling/Running a gambling place for profit

(a) Forms of offenses

In addition to "flower card" gambling, baseball gambling and game-machine gambling, there are various forms of habitual gambling/running a gambling place for profit, such as online casino gambling. The reality is that Boryokudan are directly or indirectly deeply involved in those gambling offenses, 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 2017, the orders were issued for about 192 million yen in cash in connection with illegal gambling facilities.

(b) Modus operandi of money laundering

Regarding modus operandi of money laundering offences related to habitual gambling/running a gambling place for profit as predicate offenses, there was a gambling offense committed by an online casino in which money bet by betters had to be paid to an account opened in another person's name, and there were cases of gambling offenses related to baseball gambling, etc. in which dividends were transferred to accounts in other persons' names.

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

F. 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 are certain cases where foreigners who are living illegally in Japan work illegally in adult-entertainment business, etc.

For the last three years, offenses related to violating the Amusement Business Act and the Anti-Prostitution Act rank at the top 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 modus operandi of money laundering offences related to violation of the Amusement Business Act or the Anti-prostitution Act as predicate offenses, there were cases where sales proceeds paid by credit cards were transferred to a bank account in the name of another party, proceeds paid as payback for arranging women to illegal adult-entertainment businesses were transferred to an account in the name of the offender, and where a Boryokudan member received proceeds from prostitution through a bank account in the name of a family member.

G. Narcotics-related crimes

(a) Forms of offenses

Regarding stimulant-related crimes, which account for more than 60% of all narcotics-related crimes, the amount of stimulants confiscated in 2019 was the amount seized was 2,293.1 kg, a significant increase from the previous year and the highest ever. It exceeded 1,000 kg for 4 consecutive years from 2016 to 2019, and it can be assumed that smuggling and illicit trafficking of stimulants generates a large amount of criminal proceeds.

Boryokudan gangsters, etc. accounted for at least 40% of the offenders in cleared cases of stimulant-related crimes during 2019. In terms of the number of persons cleared for stimulant-related crimes committed by Boryokudan gangsters, etc., classified by significant violation types, there were 2,117 use offenders, 1,164 possession offenders, 238 transfer offenders, 36 transfer offenders, and 36 smuggling offenders. Furthermore, of the total number of stimulant profit-making offenders cleared (682), the number of profit-making Boryokudan gangsters, etc., cleared was 276, accounting for 40.5%. The situation of Boryokudan involvement continues.

For cannabis offenders, of the total number of offenders cleared for profit-making offenders cleared (305), 99 were cleared for profit-making offenders as Boryokudan gangsters, accounting for 32.5%. Boryokudan gangsters are also involved in the smuggling of cannabis. Past research revealed that they were involved in more than 70% of large-scale cannabis cultivation for profit. It is recognized that narcotics-related crimes are one of the major sources of funds for Boryokudan gangsters, etc. Furthermore, evidence gathered in recent years strongly suggests that Boryokudan collude with overseas drug-related criminal organizations, and have been deepening their involvement in the distribution of stimulants (from shipping and receipt from overseas to central wholesale, intermediate wholesale, and distribution to end users in Japan). As of the offshore transaction of stimulant smuggling offenses, in 2017, Boryokudan gangsters and Chinese were cleared in the case of seizing about 475 kg. In 2019, Boryokudan gangsters and Taiwanese were cleared in the case of seizing about 587 kg.

As for overseas drug-related criminal organizations, Chinese, Mexican and West-African organizations have been continuing to increase their presence, and criminal proceeds from drug-related crimes are an important source of funds for overseas criminal organizations as well. A breakdown of cleared cases of stimulant smuggling by origin shows that Thailand, Malaysia, the U.S., and Canada occupy a large share in order of amounts smuggled in 2019. The breakdown of foreigners in Japan arrested for illicit stimulant trafficking by nationality shows that Iran continues to occupy a large share, and there is a threat that criminal proceeds from smuggling and illicit trafficking of drugs have been transferred between countries with different legal and transaction systems.

(b) Modus operandi of money laundering

Regarding modus operandi of money laundering offences related to illicit drug trafficking, there were many cases, including the following, where payment was concealed by remitting it to an account under the name of another person.

- Case where traffickers of stimulants by hand delivery or mail had payments transferred to an account under the name of another person
- 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

and so on.

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 arrest of the Boryokudan member and others.

Automobiles, land, buildings, etc. were also targeted for temporary restraining order for confiscation before institution of prosecution based on the previous Anti-Drug Special Provisions Law, and it is recognized that the proceeds from drug crimes 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 2017 to 2019) and counted the detected transactions etc. to be misused for money laundering while conducting criminal investigations[*1].

There were 446 cases of domestic exchange transactions[*2], 260 cases of cash transactions and 106 cases of deposit transactions that were misused of money laundering. They accounted for the majority of the transactions misused for money laundering (see Table 6).

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 as cash 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.

Table 6 [Major Transactions etc. Misused for Money Laundering (2017–2019)]

Misused transactions	Domestic exchange transactions	Cash transactions	Deposit transactions	Legal person exchange)	International transactions (such as foreign	Credit card	Electronic money	Funds transfer services	Precious metals and stones	Postal receiving service	Crypto-assets	Legal/accounting professionals	Investment	Safe-deposit box	Note/check	Insurance	Money lending	Total
Total	446	260	106	36	33	25	23	11	7	5	5	3	2	1	1	1	1	966

Typical examples of misused transactions, etc. are:

- ○ Transferring criminal proceeds from fraud to accounts held 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 from a foreign country to an account in Japan (Transactions with a foreign country)
- ○ Remitting criminal proceeds from fraud to accounts of dummy corporations (Legal persons[*3])
- ○ Selling gold ingots acquired by fraud under the name of a legal person by using 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.

---

*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 Details of cases where legal persons were misused for money laundering are explained in Legal Persons without Transparency of Beneficial Owner. in Section 5. High-risk Transactions.

Cases of misusing those transactions etc. are individually explained in *Section 4. Major Products and Services* in which Risk is Recognized.

[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, insurance companies, and credit card operators submitted STRs as below, concerning accounts (including those that were declined) of Japanese people and legal persons or contracts (including those that were declined).

- ○ Sudden large deposits and withdrawals
- ○ Many commonalities with past fraudulent accounts that business operators were aware of
- ○ Unnatural transaction content in light of the transaction purposes and occupations identified by business operators
- ○ Transactions related to Boryokudan or their associated parties

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

(2) Deposit-taking institutions, insurance companies, credit card operators, and crypto-assets exchange service providers submitted STRs as below, concerning accounts (including those that were declined) of Japanese people and legal persons, or contracts (including those that were declined).

- ○ Frequent transfers from a large number of people, followed by withdrawals
- ○ Quick representatives change after the establishment of the corporations, and the actual business situation was unclear
- ○ 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 in loan sharking. The holders and users (Boryokudan members) of those accounts were cleared in violation of the Money Lending Business Act (unregistered business operation) and the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

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

A deposit taking institution submitted STRs as below concerning a foreigner's account.

- ○ Frequent remittances in a short period
- ○ Frequent remittance transactions with specific accounts
- ○ Unnatural transaction content in light of the transaction purpose and occupation declared at the time of opening the account
- ○ Remittances from multiple foreigners, followed by transfers to crypto-assets exchange service providers
- ○ Frequent transfers from an unspecified number of individuals, after which most were withdrawn
- ○ The occurrence of transactions that deviated from the past transaction behavior

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

3. Cases of Violating the Stimulant Control Act

Deposit-taking institutions, credit card operators, and crypto-assets exchange service providers submitted STRs as below, concerning accounts of Japanese or contracts (including those that were declined).

- ○ Frequent transfers from multiple people, followed by withdrawals
- ○ Frequent remittance transactions involving large numbers of people and large amounts of money
- ○ Suspicious situation where those who apply for transaction frequently talk to someone on the mobile phone
- ○ Frequent remittances in a short period
- ○ Large amounts of cash transactions
- ○ Unauthorized use of stolen cards
- ○ Transactions related to Boryokudan or their associated parties

With the above as a starting point, those concerned (Boryokudan or affiliated members), including the account holder (a Boryokudan member), were cleared for violating the Stimulant Control Act (Act No. 252 of 1951) (account transferred for profit).

4. Fraud Cases

Deposit-taking institutions and fund transfer service providers submitted STRs as below with respect to accounts of foreigners (including ones that were declined).

- ○ Remittance to countries that the business operators have designated as high-risk countries
- ○ Large amounts of withdrawals from ATMs
- ○ Frequent remittances in a short period
- ○ Frequent remittance transactions involving large numbers of people and large amounts of money, and subsequent withdrawal
- ○ Cash withdrawals after a large number of sudden transfers, and no rationality is seen considering the transaction purposes, customer attributes, etc.
- ○ Large amounts of unnatural remittances/transfers (including remittances from foreign countries)
- ○ Documents to confirm the transaction details were returned because the addresses were unknown.

With the above as a starting point, it was discovered that several people involved, including the account holder, were tricking a woman into transferring cash to the account, and the account holders were cleared for fraud.

5. Cases of Official Stamped Document and Private Document Forgery and Execution, and Fraud

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

- ○ Card application by spoofing
- ○ Opening accounts and applying for loans with forged driver's licenses
- ○ Large amounts of remittances from specific people, and subsequent withdrawal
- ○ Suspicion of using fictitious names or other people's names
- ○ Large amounts of cash transactions
- ○ Unnatural transaction content in light of the transaction purpose and occupation declared at the time of opening the accounts
- ○ The same mobile phone numbers as the registered phone numbers of other peoples' accounts reported
- ○ The same e-mail addresses as the registered e-mail addresses of other people's accounts reported

With the above as a starting point, it turned out that some of accounts opened and credit card contracted were fraudulently made, and with forged drivers' licenses. Those who opened (contracted) were cleared for official stamped document and private document forgery and execution and fraud.

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

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

- ○ Cash transactions intentionally distributed in small lots
- ○ The unnatural usage pattern of accounts despite being office workers, such as requesting the collection of a large number of bills and checks using their accounts
- ○ Large amounts of transfers from multiple individuals

With the above as a starting point, it turned out that the accounts were used for loan sharking. Several related parties, including the account holders, were cleared in violation of the Money Lending Business Act (no documents issued) and the Investment Act (high interest rates).

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

- ○ Frequent remittances in a short period
- ○ Large amounts of cash transactions and remittance transactions
- ○ Suspicious remittance requesters
- ○ Transactions related to Boryokudan or their associated parties

With the above as a starting point, suspicious transfers of funds related to the accounts were found. The account holders were cleared in violation of the Money Lending Business Act (unregistered business).

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

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

- ○ Frequent remittance transactions with many people, including specific people, followed by withdrawals
- ○ Reports on fraud damage from customers who made transfers to the accounts

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 cleared for fraud.

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

- ○ Application for opening accounts with the same email addresses as other people
- ○ Frequent remittances from many people
- ○ Many transfers within a certain period, followed by withdrawals from ATMs
- ○ Existence of other accounts related to holders with their accounts frozen
- ○ Sudden remittances from multiple individuals, followed by immediate withdrawals at remote locations

With the above as a starting point, some accounts were found to be used by third parties. The account holders were cleared for the fraudulent opening of the accounts to transfer them to others.

The accounts were used for specialized fraud.

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

- ○ A large amount of money transferred from individuals to accounts that have not been traded for a certain period, followed by withdrawals
- ○ Existence of other accounts related to holders with their accounts frozen
- ○ Repeated transfers from specific people, followed by withdrawals
- ○ Use multiple accounts with different account holder names

With the above as a starting point, some accounts were found to be used by third parties. The account holders were cleared in violation of the Act on Prevention of Transfer of Criminal Proceeds (transfer, etc., of deposit passbook, etc.).

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

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

- ○ No transactions corresponding to the transaction purpose declared at the time of opening the account
- ○ Large amounts of cash deposits and transfer deposits with no proper reasons confirmed in light of the customer attributes
- ○ A large number of sudden transfers and cash deposits with no proper reasons for the rapid increase in transactions

With the above as a starting point, the account holder's activities outside the status of qualification were found. They were cleared in violation of the Immigration Control and Refugee Recognition Act (activity outside the qualification status).

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

- ○ Use of the accounts far away from the registered addresses
- ○ With fraudulent damage reported from other customers who made remittances to the accounts, the transfer was almost fully withdrawn at the ATM after deposits
- ○ Mail sent to the registered addresses returned due to no existence of the addresses

With the above as a starting point, it was found that the account holder had a forged residence card and was cleared in violation of the Refugee Recognition Act (possession of a forged residence card).

Section 4. 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 2020, there are 1,344 institutions that have obtained the licenses, etc. They are mainly banks (136 banks, except branches of foreign banks) and cooperative financial institutions (255 Shinkin Banks, 145 Credit Cooperatives, 13 Labour Banks, 680 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 818.2504 trillion yen as of the end of September 2019.

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 authorities overseeing deposit-taking institutions, 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) for supervision. 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. Each regional bank and regional bank II have a certain geographic area where it mainly operates, 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 passed funds illegally obtained by fraud, etc. in foreign countries through Japan's financial institutions as part of their money laundering process.

In addition, with respect to transactions, excluding cash deals, that were illicitly used for money laundering in the past three years, domestic exchange transactions, deposit transactions and transactions with foreign countries (foreign exchange transactions, etc.) handled by deposit-taking institutions actually account for almost all of them. Elements that influence risks related to deposit and savings accounts, deposit transactions, domestic exchange transactions, safe-deposit boxes, bills, and checks that comprise the products and services handled by deposit-taking institutions are as described below.

---

*1 This NRA-FUR lists products and services according to the type of business operator. However, each business operator covers different scopes of products/services. Business operators are required to consider the related contents in this NRA-FUR based on products/services they deal with.

*2 Deposit-taking Institutions mean those listed in Article 2, paragraph 2, items 1–16 and 36 of the Act on Prevention of Transfer of Criminal Proceeds (banks, Shinkin banks, etc.).

*3 See FY2019 Interim Financial Statement Analysis of All Banks by Japanese Bankers Association (covers 114 banks).

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

Due to the above characteristics, the Financial Services Agency evaluates that ML/TF risks for the business type of deposit-taking institutions is higher than that for other business types. The Financial Services Agency is requesting financial institutions that handle deposits to upgrade their AML/CFT systems. The Financial Services Agency evaluates that the level of the overall system is improving. Still, the efforts of some deposit-taking institutions were delayed through the supervision so far. Some deposit-taking institutions in which risk identification or assessment and ongoing CDD are insufficient. However, as of risk identification and assessment, such as those of products and services they provide, transaction types, countries and regions related to transactions, and customer attributes. After that documents prepared by specified business operators have begun to permeate all deposit-taking institutions. Items related to risk identification and assessment and analysis contents in documents prepared by specified business operators have also been improved. Regarding ongoing CDD, which is vital as measures to mitigate risks, it is said that efforts toward the implementation of customer risk assessment have become widespread.

(b) Trends of STRs

The number of STRs submitted by deposit-taking institutions was 1,093,700 between 2017 and 2019, accounting for 86.9% of total reports.

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

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

- Unusual transactions or transactions related to customers who show unusual behavior or movements, based on the knowledge and experience of staff (208,514 reports, 19.1%)
- Transactions related to Boryokudan or their related parties (148,599 reports, 13.6%)
- Transactions in which a large amount of money is transferred from foreign countries without an economically justifiable reason (78,701 reports, 7.2%)
- Transactions involving deposits or withdrawals (including trade of securities, remittance, and currency exchange; hereinafter, the same applies) using large amounts in cash or checks. In particular, high-value transactions that were disproportionate to the customer's income or assets, or transactions in which deposits or withdrawals dare to be made in cash even though use of a remittance or cashier's check is considered to be more reasonable (78,613 reports, 7.2%)
- Transactions using accounts that frequently receive remittances from many persons. In particular, cases where an account receives a remittance and a large amount of money is transferred or paid from the account immediately after receiving such remittance (75,436 reports, 6.9%)
- 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 (74,698 reports, 6.8%)
- Transactions for which a large amount of money is transferred to foreign countries without an economically justifiable reason (46,928 reports, 4.3%)
- Transactions related to accounts through which a large amount of money is frequently deposited or withdrawn (38,377 reports, 3.5%)
- 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 (38,109 reports, 3.5%)
- Deposits or withdrawals using accounts suspected to be opened in a fictitious or other person's name (35,561 reports, 3.3%)

---

*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.

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) Products/Services Provided by Deposit-taking Institutions

(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 store verification records and transaction records when they conclude deposit/savings contracts (contracts for the receipt of deposit/savings) with customers. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

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 followings are examples of cases where deposit/savings accounts were misused for money laundering:

- Case where accounts belonging to deceased persons or foreign nationals who have returned to their home countries were used due to the failure to close such accounts, and in which criminal proceeds from fraud, theft, etc. were concealed
- Case where offenders received or concealed criminal proceeds derived from fraud, theft, loan-shark crime, drug crime, violation of the Amusement Business Act, 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

and so on.

Most misused accounts are those under the name of an individual. There are various means of illegal acquiring accounts: borrowing a family member or friend's account; purchasing one from a third party; and opening one under a fictitious name. Certain characteristics can be identified, such as accounts under the name of the debtor for a loan-shark being used for loan-shark crimes, Boryokudan members using accounts under the name of a family member or friend in the case of 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.

- There are cases where dozens of other people's passbooks and cash cards, most of which belonged to foreigners, were seized from the suspect's home in a fraud group cleared 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, misusing accounts under corporate names is characteristic of crimes committed by organized crime groups that generate large amounts of proceeds, such as specialized fraud or cross-border money laundering cases.

In this way, accounts opened under fictitious names or in the names of third parties are obtained through illegal trading and misused to receive criminal proceeds in specialized fraud, loan-shark cases, etc. Proceeds are transferred through 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.

- ○ A case of seizing hundreds of passbooks from the criminal base of a foreigner visiting Japan, who was cleared for illegally soliciting the transfer of accounts by posting the solicitation on an SNS as buying bank accounts, passbooks, cards, etc.

Many cases have been cleared. Chart 7 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 various cases, the number of accounts being significantly transferred exceeds the number of cleared cases. It should be noted that the transfer of accounts encourages the deeds of ML/TF. Furthermore, looking at the number of cleared cases by nationality, Japan has the most, followed by Vietnam, and China. Compared to the number of foreign residents in Japan, it can be said that the occurrence of account transfers involving foreigners is conspicuous.

In addition, the police are also taking the initiative in investigating cases of account fraud, in which offenders cheat deposit-taking institutions out of deposit/savings passbooks by falsely representing the location of a postal receiving service provider as their address when opening an account (account fraud), for example, while concealing the purpose of transferring the account to others, and cases of receiving a passbook knowing that these are obtained illegally, applying the provision of receiving stolen property (see Table 8).

Table 7 [Number of Cleared Cases of Violating the Act on Prevention of Transfer of Criminal Proceeds (2017–2019)]

Category \ Year	2017	2018	2019
Transfer of deposit/savings passbook, etc.	2,523	2,519	2,479
Transfer of deposit/savings passbook, etc. (business)	27	27	44
Solicitation for transfer of deposit/savings passbooks, etc.	31	27	27
Transfer of exchange transaction cards, etc.	0	0	27
Transfer of information for crypto-assets exchange	0	2	0
Others	0	0	0
Total	2,581	2,575	2,577

Table 8 [Number of Cleared Cases of Account Fraud etc. (2017–2019)]

Category \ Year	2017	2018	2019
Account fraud	1,512	1,277	919
Transfer of stolen goods	6	4	6
Total	1,518	1,281	925

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 due to cooperation between deposit-taking institutions and around-the-clock convenience stores, transactions related to deposits or withdrawals of deposit/savings (hereinafter referred to as "deposit transactions") provide high convenience to account holders. People can withdraw or deposit funds quickly and easily, regardless of the time and place.

On the other hand, those who attempt money laundering, etc. pay attention to safe and reliable management of funds and high convenience of deposit transactions that accounts provide, and attempt to launder money through depositing and withdrawing the proceeds of crimes.

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). The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

b. Typologies

The following cases are examples of misusing deposit transactions for money laundering:

- Case where 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
- Case where an offender concealed criminal proceeds derived from theft, fraud, embezzlement, drug crime, gambling, etc., by depositing them into accounts opened in another person's name
- Case where 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 it in bills at another ATM
- Case where a Vietnamese offender transferred proceeds from underground banking into an account of his relative who had become naturalized as Japanese and has a Japanese name
- Case where an offender deposited cash into an account under the name of his relative immediately after committing a crime for fear of the crime being detected due possessing the cash, and subsequently withdrew the money
- Case where an offender deposited some of the cash obtained through armed robbery into an account multiple times in a short period under the name of his acquaintance via an ATM

and so on.

(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 verification at the time of transactions, and to prepare and preserve verification records and transaction records when they conduct receipt or payment transactions of cash that exceed 100,000 yen, including exchange transactions. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of

this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the mode of ordinary transactions and the like. In addition, in the case of domestic exchange transactions involving the payment of funds to other financial institutions, when the receiving financial institutions ask the paying financial institutions to conduct customer identification related to the transactions, the Act obligates the paying financial institutions to prepare records on matters that enable the search of the customers' records to be verified within three business days of the request date, and obligates the receiving financial institutions to prepare records concerning matters that enable a search of information concerning the transactions.

b. Typologies

The following cases are examples of misusing domestic exchange transactions for money laundering:

- Case where a senior Boryokudan member received criminal proceeds, which were derived from fraud by his acquaintance, by making the acquaintance remit to the member's account
- Case where 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
- Case where an offender took requests from more than one client and had them remit cash for an illegal overseas transfer of money into an account that the offender had acquired from a returned Vietnamese in return for remuneration
- Case where 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
- Case where 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
- Case where a Chinese offender engaging in agriculture in Japan obtained criminal proceeds by having Chinese worker without a work qualification certificate work illegally through remittances to an account under the name of Chinese whom hired before.
- Case where an offender made the victim remit cash defrauded from him by specialized fraud to an account in another person's name, and then transferred it into the account under his name that had been opened in advance for the purpose of concealing criminal proceeds
- Case where 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 a work qualification certificate to factories
- A case where the money obtained from a fraudulent internet auction was transferred to an acquaintance's account in online bank that had been opened in advance to conceal criminal proceeds

and so on.

(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. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

b. Typologies

The following cases are examples of misusing safe-deposit boxes for money laundering:

- Case where an offender cheated a victim out of his 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 his relative
- Case where criminal proceeds derived from fraud cases were contributed 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

and so on. Also, in foreign countries,

- Case where an offender concealed criminal proceeds by using false names to lease safe-deposit boxes at many banks

Thus, actual situations exist where persons attempting to commit ML/TF misuse safe-deposit boxes as a physical means of storing criminal proceeds by leasing safe-deposit boxes using other people's names while concealing the real user.

(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[*1] or checks drawn to self[*2] 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). The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

Furthermore, 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 verification at the time of transactions when opening accounts.

---

*1 Checks drawn as bearer checks stipulated in Article 5, paragraph 1, item 3 of the Check Act (Act No. 57 of 1933) or checks deemed to be bearer checks pursuant to the provision of paragraph 2 or 3 of said Article and not crossed under Article 37, paragraph 1 of the Act.

*2 Checks drawn to self, pursuant to the provision of Article 6, paragraph 3 of the Act and not crossed under Article 37, paragraph 1 of the Act.

b. Typologies

The following case is an example of misusing bills and checks for money laundering in Japan:

- Case where bills or checks were misused for money laundering, including a case where 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

and so on. Also, in foreign countries,

- Cases where bills or checks were misused to smuggle huge amounts of funds
- Cases where bills or checks were misused by drug cartels as a way to separately transfer a huge amount of money

and so on. 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.

B. Measures to Mitigate Risks

(a) Statutory measures

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

Moreover, in addition to supervisory measures based on the Act, the Banking Act provides that the competent authorities may require submission of reports from, issue business improvement orders to, and conduct on-site inspection of, banks if necessary. 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. After that the Agency revised part of the Guidelines in April 2019 to clarify that risk assessment should be conducted for all customers, etc. and thereby has established an effective system for implementing AML/CFT measures among financial institutions, etc.

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 contracts, 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 state and Guidelines. Then the Agency provides guidance or supervision, etc. corresponding to risks of business operators based on the assessment results.

Consequently, it is made clear that although preparation of the document prepared by specified business operators is conducted by many business operators, the sufficiency of the content of the document varies by business operator and that, although risks peculiar to local financial institutions are not so different from those of major banks, efforts toward a risk-based approach are quite different. Taking these points into account, the Financial Services Agency requires all business operators, regardless of their size, to implement risk assessment. The Agency provides guidance for and supervision of their efforts toward implementing the risk-based approach, including establishing and maintaining, etc. an internal control system, by not simply

---

*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.

focusing on formally checking for the existence of violations 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 Agency has also been considering issues common to a wide range of business categories, such as shared operation of systems, as issues common among financial institutions.

Furthermore, in cooperation with industry associations and the Finance Bureau, the Financial Services Agency continuously provides lectures and training to financial institutions to improve AML/CFT measures. In 2019, 85 lectures and training were given, including those to other types of businesses. They are 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.

The Ministry of Agriculture, Forestry and Fisheries and the Ministry of Health, Labour and Welfare also performs documentary research and issues report submission orders to grasp the actual situation of compliance with laws and regulations and risk control by business operators. The Ministries also provide guidance and supervision, etc. corresponding to the risks of respective business operators based on information obtained through such research and orders.

The following matters are those identified by the competent authorities that business operators should note:

- Matters with management involvement
  - While management proactively and independently conduct themselves, give specific instructions and foster collaboration, etc. among relevant departments, business operators should develop effective risk mitigation measures and action plans. At the same time, from the perspective of system development, it is necessary to promote company-wide measures by grasping appropriate management resources and reviewing system development.
  - The administrative division must, in addition to distributing the List of Reference Cases of Suspicious Transactions released by the Financial Services Agency to sales offices, communicate to all sales offices specific examples that take into account risks that they may face, and establish a system that enables them to detect suspicious or abnormal transactions.
  - The administrative division must verify the detection status of suspicious or abnormal transactions at sales offices and overseas transmittance divisions, and it is necessary to verify the effectiveness of the management system on a risk basis.
  - In addition to rules-based internal audits, internal audits based on 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.
- CDD measures
  - 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.
  - Sharing information with sales offices, etc. because some business operators repeatedly accept transactions that are similar to ones that were reported as suspicious transactions in the past.
  - Certain measures are being taken to prevent anti-social forces (Boryokudan, etc.) from opening accounts, and to close their accounts that are already open. Furthermore, it is important to also monitor and filter transactions such as remittances carried out by anti-social forces (Boryokudan, etc.) that have existing bank accounts, and consider submitting STRs.

- With regard to foreigners, grasping their period of stay, informing them when they open an account that trading of accounts is a crime and influencing them to close their accounts when returning home, etc., and detecting possible cases of illegal/unauthorized use of the accounts.
- When opening an account of a foreigner, if the katakana name and alphabetic name is written on the customer identification documents, customer attribute of each name should be confirmed.

○ Transaction monitoring and notification of suspicious transactions

- For transaction monitoring, it is necessary to set a scenario based on the own ML/TF risks, and consider other risks so that the monitoring targets are not biased toward specific financial crimes, such as specialized fraud cases.
- Regarding transaction monitoring, it is necessary to set threshold values according to the customer risk assessments and regularly review 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
- For STRs, establish a system for appropriate examination and judgment, and utilize the status of STRs to strengthen an own risk control system.

○ Matters regarding performance of 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 customer attributes of a person responsible for a transaction who visits the bank teller (verification as to whether the person falls under anti-social forces, etc.) at the time of opening an account
- 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

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

(c) Measures by industry associations and business operator

Regarding industry associations, they support the AML/CFT measures of each business operator by providing case examples, supplying a database on subjects such as freezing assets, and offering training, etc. In particular, the Japanese Bankers Association (JBA) continuously follows up on the FATF's considerations on money laundering, etc. In addition, the JBA continually exchanges information with overseas banking associations and the like, and responds to the FATF's reciprocal examinations of Japan 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.

Business operators themselves are endeavoring to establish and reinforce their own AML/CFT internal control systems, too. For example, some have set up a division in charge, developed internal regulations and

manuals, and carry out periodic training, 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 efforts to implement the risk-based approach taken by business operators:

- For those related to risk identification
  - Cases where a company analyzes STR(s), and extracts an independent risk index from trends for countries and areas of destination and origin regarding overseas remittances, trends for nationalities regarding accounts by the names of foreigners, and trends for occupation or type of business with respect to customers
  - Cases where a transaction related to a business that handles products possibly used for military purposes is specified explicitly as a high-risk transaction with consideration of information published by competent authorities.
  - Cases where a company, not only by considering direct descriptions in the NRA-FUR, but also by taking into account the principle of the descriptions, identifies specific risks where foreigners who are assumed to be returning home, such as students studying in Japan or short-term employees, may sell their accounts illicitly at the time of return, or operators who handle cash in a concentrated manner may receive a mixture of unauthorized funds in transactions.
  - Cases where transactions using ordinary deposit accounts under foreigners' names, in which movements such as salary transfers stopped or corporate accounts that were opened by applying at the teller but for which the actual activities of the corporation could not be sufficiently grasped at on-site visits, are specifically identified as high-risk transactions.
- For those related to risk assessment
  - Cases where domestic exchange transactions are segmented into general transfers, salary transfers, tax payments, public utility charges, outward remittances, incoming remittances and so on, and risks of each segment are assessed.
  - Cases where a customer reported with STRs in the past is evaluated as high-risk customer according to the content of the notification.
  - 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.
  - Cases of correspondent management where risk is evaluated by focusing on the correspondent's business area, attributes, business content, and the presence or absence of disposal related to ML/TF.
- For those related to the risk-based approach
  - Cases of a customer who was reported with STRs in the past, where an information-sharing system is established and when dealing with the customer. Details are confirmed by checking the documents and interviewing and then transaction is approved by the senior manager.
  - Cases where 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 a category, 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 the senior administrator's confirmation.
  - Cases of banks that have an internal regulation system whereby accounts opened with a small amount of money, 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 targeted for control. If any request for a transfer to such accounts occurs, the consistency of such request with the purpose of opening the account is checked and the intent of the person requesting the transfer is checked, and if the consistency cannot be confirmed, the transaction is denied or the transaction is reported as suspicious.

- Cases where misuse of bank accounts is prevented by stopping accounts in which deposit and withdrawal transactions are absent for a long time and checking the principal identification documents, passbooks, etc. of customers who wish to resume transactions.
- Cases of checking the visa length of customers who are foreign students or workers, and using a system to control the risk of sale of accounts at the time of their return home.
- Cases where corporate customers that newly start foreign exchange transactions are visited on-site by the headquarters and a responsible person at the sales office before stating transactions, 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 when a request is made.
- Cases where the case-by-case approval process is clear whereby, for example, a checklist for foreign remittances is prepared, and a teller of a branch office performs checks based on the list, and a general manager verifies and reports to the responsible division at headquarters.
- Cases where a business operator's environment, strategy, geographical characteristics in the sales area, and its customers' characteristics are analyzed to extract unique risk indicators from the geographical characteristics of business areas, such as being close to airports and ports. The business operator identifies vendors that may dismantle, purchase, 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.
- Cases where handling overseas remittances with cash brought in is suspended.
- Cases of non-face-to-face transactions, where transaction monitoring is conducted focusing on access information, such as IP addresses and browser languages, with consideration of the possibility of spoofing.

C. 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, statistics of transactions misused for ML/TF, occurrences of 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.

---

*1 Article 2, paragraph 2, item 35 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.

*2 Article 2, paragraph 2, item 27 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.

Competent authorities and operators are taking, statutory measures as a matter of course, the above-mentioned mitigating measures against these risks, and the outcomes of such measures can be seen from the way operators are effectively managing the risks.

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole. Most of the concealment cases of criminal proceeds in 2019 used a method of money transfer to third-party accounts. There were more than a dozen accounts of others abused in some cases. Furthermore, hundreds of passbooks were seized from the crime base of a person cleared for soliciting the transfer of accounts. Accounts in others' names are the main criminal infrastructure, such as ML/TF. Business operators who provide the account must take continuous measures to prevent the transfer of accounts and take ex-post-facto detection measures.

In addition, based on STRs and actual cases, it is recognized that transactions that involve the following transaction conditions, customer attributes, etc., the following items are recognized as having an even higher risk regarding the situation at the time of transaction and the attributes of customers, besides the transactions specified in 5. High-risk Transactions.

- Transactions under anonymous or fictitious names, borrowed names, and false names (including suspected ones)
- Transactions made by numerous people
- Frequent transactions
- Large amounts of remittance and deposit or withdrawal transactions
- Transactions where sudden large deposits and withdrawals are made despite accounts that normally do not move funds
- Transactions, including 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.
- 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 2020, there were 95 companies that had obtained a license from the prime minister based on the Insurance Business Act (Act No. 105 of 1995).

(b) Trends of STRs

The number of STRs submitted by insurance companies, etc. between 2017 to 2019 was 7,929 (7,050 reports for life insurance, 814 reports for general insurance, and 65 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 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 or their related parties (5,750 reports, 81.6%)

And cases for general insurance are as follows.

- Transactions related to Boryokudan or their related parties (479 reports, 58.8%)
- Unnatural transactions or transactions related to customers who show unnatural behavior or movements based on the knowledge and experience of staff (41 reports, 5.0%)

Furthermore, in the life insurance sector, there was a certain number of STRs focusing on payment of premiums in a large amount of cash (13 reports, 0.2%), including an STR where a customer made a lump-sum payment in cash (15 million yen) for a premium.

(c) Typologies

The following case is an example of misuse of insurance for money laundering abroad:

- Case where a drug trafficking organization spent its drug proceeds on the purchase of life insurance, then soon afterward cancelled the insurance and received a refund

and so on. The following case is an example of criminal proceeds being transformed in Japan:

- Case where criminal proceeds derived from fraud and prostitution were spent on the purchase of installment life insurance for offenders and their family members

---

*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.

The case specified below is an example of insurance related to money laundering.

- Case where deceived non-life insurance money was transferred to an account in the name of another person

and so on.

B. 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. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

Moreover, in addition to the supervisory measures based on the Act, the Insurance Business Act provides that competent authorities can order the submission of reports from, issue business improvement orders to or conduct on-site inspection of insurance companies 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 that business operators, etc. 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 Financial Services Agency conducts documentary research and issues report submission orders, and uses gap analysis, etc. to perform risk assessments on the types of businesses or operators based on the Guidelines mentioned above, and provides guidance or supervision, etc. corresponding to the risks of operators based on the assessment results.

Furthermore, in cooperation with industry associations and the Finance Bureau, the Financial Services Agency continuously provides lectures and training to financial institutions to improve AML/CFT measures. In 2019, 85 lectures and training were given, including those to other types of businesses. They strive 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.

The following matters are those identified by the competent authorities that business operators should note:

- Comprehensively 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 involving in transactions, and customer attributes when preparing or reviewing the document prepared by specified business operators
- Establishing a system for verification at the time of transaction according to the risk and ongoing CDD
- 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
- Complying with domestic and foreign laws and regulations related to sanctions, taking other necessary measures, and building a framework to detect high-risk customers accurately

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

(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.

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 internal regulations and manuals, provide periodic training, conduct internal audits, screen out transactions that are considered to be high risk, and adopt enhanced monitoring of high-risk transactions.

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

- Cases where the inherent risk associated with cash transactions is regarded as high risk and thereby the receipt of cash for insurance premiums, repayment of loans to policyholders, etc. is canceled; as a rule, cashless insurance payment is also promoted by making payments to the accounts of the principals for which money is held; when a cash transaction exceeds a certain amount, a questionnaire, etc. using specified check sheets, etc. is conducted and the approval of a supervisor is required; and transaction conditions, etc. are captured by the system in order to manage them after the fact

C. Assessment of Risks

Since insurance products with cash accumulation features enable ML/TF 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 operators are taking, statutory measures as a matter of course, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole.

In addition, based on STRs, actual cases, etc., it is recognized that transactions that involve the following transaction conditions, customer attributes, etc., the following items are recognized as having an even higher risk regarding the situation at the time of transaction and the attributes of customers, besides the transactions specified in 5. High-risk Transactions in this survey.

- Transactions under anonymous or fictitious names, borrowed names, and false names (including suspected ones).
- If an insurance premium is paid at the time of concluding a contract and then the contract is canceled promptly, the risk is considered to be particularly high.

(3) Investment 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, investment in stocks, bonds, and other investment products are also useful ways to manage funds. Investment instruments include commodity derivatives transactions in minerals and agricultural products, as well as financial products such as stocks, bonds, and investment trusts.

As of the end of March 2020, there were 4,585 business operators registered by or notified to the prime minister based on the Financial Instruments and Exchange Act (Act No. 25 of 1948) and 41 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).

Upon surveying investment transactions in Japan, the total transaction volume of stocks listed on the Tokyo Stock Exchange, Inc. (First Section and Second Section) was about 604.4022 trillion yen in 2019 (see Table 9).

Regarding commodity derivatives transactions, the trading volumes at commodity exchanges in Japan (Tokyo Commodity Exchange, Inc. and Osaka Dojima Commodity Exchange) were about 19.31 million sheets[*2] in 2019. The total value was about 55.5184 trillion yen in 2019, and the clearing-margin balance at the end of December was about 134.9 billion yen (see Table 10).

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 the criminal proceed if criminals deposit funds or commodities or make investments and convert a large amount of money into various commodities or make investments in commodities 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, in the provision of deposit and withdrawal services linked to bank accounts, there is a risk that necessary confirmations will be insufficient due to the speeding up of fund transfer. Furthermore, it is said that there is a risk that unlawful acts, such as insider trading, will be conducted in the process of investment. The funds generated from the illegal acts will be combined with legal assets, or the investment will be used to raise funds for antisocial forces. In non-face-to-face transactions, there is a risk of dealing with a fictitious person or a person impersonating another person.

Table 9 [Transaction Volume of Stocks (2017–2019)]

(Unit: million yen)

Year / Category	2017	2018	2019
First Section, TSE	683,218,254	740,746,041	598,213,662
Second Section, TSE	12,744,471	11,006,506	6,188,491
Total	695,962,725	751,752,547	604,402,153

Note: Data from the Tokyo Stock Exchange

---

*1 Financial instruments business operators, etc. and commodity derivatives business operators mean those listed in Article 2, paragraph 2, item 21 (financial instruments business operators), item 22 (securities finance companies), item 23 (special business notification persons), and item 32 (commodity derivatives business operators) of the Act on Prevention of Transfer of Criminal Proceeds.

*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.

Table 10 [Transaction Amount of Commodity Derivatives Transactions (Domestic Commodity Exchanges) (2017–2019)]

Category \ Year		2017	2018	2019
Volume (number of contracts) (Sheet)	Agricultural products	665,435	416,927	391,409
	Minerals	23,866,328	23,443,439	18,914,218
Transaction amount (100 million yen)		517,754	585,971	555,184
Margin balance (end of December) (100 million yen)		1,773	1,257	1,349

Note 1: Data from Japan Commodity Clearing House Co., Ltd.
2: Agricultural products in the volume column is the total transaction volume of the agricultural product market, fisheries market, agricultural products index market, and sugar market. Minerals is the total transaction volume of the rubber market, precious metals market, oil market and Chukyo Oil Market.

(b) Trends of STRs

The numbers of STRs submitted by financial instruments business operators and commodity derivatives business operators between 2017 and 2019 were 38,897 and 323, 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 major ones by number of reports for financial instruments business operators, etc. are as follows.

- Tradings of stocks, securities, and investments in investment trusts, etc., using accounts suspected to be opened by a fictitious person or in another person's name (10,833 reports, 27.9%)

And, in the case of the commodity derivative business operators are as follows.

- Transactions in which it was suspected that the customer was using a fictitious or other person's name (167 reports, 51.7%)

(c) Typologies

The following case is an example of misusing investment for money laundering through financial instruments business operators, etc. and commodity derivatives business operators:

- Case where an offender remitted criminal proceeds derived from fraud into an account in a securities company that was opened under a false name, and the offender purchased stocks

and so on. Meanwhile, the following case is an example where criminal proceeds were transformed.

- Case where criminal proceeds derived from embezzlement were invested in commodity derivatives

and so on.

B. 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 who handle investment instruments to conduct verification at the time of transactions, and produce and preserve verification records and transaction records when opening accounts, when conducting transactions of financial instruments, or at commodity markets, etc. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

Furthermore, in addition to the supervisory measures under the Act, the Financial Instruments and Exchange Act and the Commodity Derivatives Act provide that competent authorities may conduct on-site inspection of, require submission of reports from, or issue business improvement orders, etc. to business operators 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 and grasp the current state of compliance with laws and regulations and of risk control. The Financial Services Agency conducts documentary research and issues report submission orders, and uses gap analysis, etc. to perform risk assessments on the types of businesses or operators based on the Guidelines mentioned above, and provides guidance or supervision, etc. corresponding to the risks of operators based on the assessment results. Furthermore, as a part of its year-round monitoring activities for financial instruments business operators, etc. the Financial Services Agency verifies the current status of measures taken for ML/TF.

Furthermore, in cooperation with industry associations and Local Finance Bureaus, the Financial Services Agency continuously provides lectures and training to financial institutions to improve AML/CFT measures. In 2019, 85 lectures and training were given, including those to other types of businesses. They are 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. For example, at a seminar hosted by the Investment Trusts Association, Japan and the Japan Investment Advisers Association, the Financial Services Agency explained the current status and issues of dealing with ML/TF in the investment management industry. The Securities and Exchange Surveillance Commission annually publishes the *Securities and Exchange Surveillance Overview and Casebook*, which introduces examples of inadequate internal control systems related to ML/TF.

The Ministry of Agriculture, Forestry and Fisheries, and Ministry of Economy, Trade and Industry have clarified the basic concept of effective AML/CFT measures and, from the perspective of encouraging commodity derivatives business operators under their jurisdiction to put effective measures in place, released the Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in the Commodity Derivatives Business in August 2019, requested operators to establish and maintain risk management systems for ML/TF based on the Guidelines, and grasp the actual situation with regard to legal compliance and risk management by commodity derivatives business operators 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 ML/TF. The Ministry of Land, Infrastructure, Transport and Tourism, etc. also undertakes documentary research and issues report submission orders to grasp the actual status of compliance with laws, regulations, and risk control by specified joint real estate enterprises, etc. and it provides guidance and supervision corresponding to risks of respective enterprises based on information obtained through the research and issued orders.

The following matters are those identified by the competent authorities that business operators should note:

- 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.
- For purpose of preparing the document prepared by specified business operators 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 document prepared by specified business operators.
- 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.

- ○ 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 customers 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.
- ○ For customers who have declared that they fall under foreign PEPs, take appropriate measures such as enhanced CDD after checking the relevant details.
- ○ 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.
- ○ For remittances from people with different accounts or withdrawal to those with different accounts or for transactions with a transfer of the value of property such as a transfer of securities, etc. between accounts under different persons' names, take appropriate measures such as checking the reasons for the transactions as necessary and checking for the presence or absence of any suspicious transactions.
- ○ In the case of allowing high-value cash transactions at store counter, confirm and record the reasons for using such transactions and the payment route (whether the customers' funds, etc.), 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 due to the 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.
- ○ For suspicious transactions that are suspected of being wash sales, etc. according to inquiries from overseas regulatory authorities, take appropriate measures such as submitting 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,

and so on. The competent authorities are making improvements and corrections with respect to these matters by providing instructions, etc. to business operators.

(c) Measures by industry associations and business operator

The Japan Securities Dealers Association[*1], the Commodity Futures Association of Japan[*2], and Type II Financial Instruments Firms Association created Q&As or other materials regarding the Act on Prevention of

---

*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 2020, 266 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.

Transfer of Criminal Proceeds, etc. and held training seminars in 2019 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' notifications of suspicious transactions and strive to make appropriate notifications. This guide has been prepared by the Association and 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 training 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.

The Investment Trusts Association, Japan has been following 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. Using the Guidelines, the Association has created a practical manual for members on AML/CFT measures at investment trust management companies and asset management companies operated by investment trust companies. From the viewpoint of the efficient implementation of the measures, an expert committee was set up in the Association in September 2019 to support the promotion of the initiatives.

The Association for Real Estate Securitization supports its members in taking AML/CFT measures by preparing a handbook with an overview of the Act on Prevention of Transfer of Criminal Proceeds, distributing a summary of matters to check at the time of transaction, etc.

Business operators themselves are also taking measures to establish and strengthen their AML/CFT internal control systems. For example, they have set up a division in charge, and develop their own rules and manuals, provide periodic training, conduct internal audits, screen out transactions that are likely to pose ML/TF risks, and rigorously conduct CDD.

Furthermore, with respect to investments conducted through financial instruments business operators, etc. (sale and purchase of securities and other transactions), it is stipulated in operators' general conditions or other documents that in principle, customers are allowed to transfer funds only to accounts with their own name, but not to third parties. This can be considered as a measure to mitigate the investment risk if remittance and payment by different names is properly controlled.

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

- The confirmation and management of foreign customers' period of stay, the confirmation of the beneficial owners of legal persons using a third-party information agency, and freezing and transaction suspension of non-operating accounts as an example of enhanced customer due diligence.
- An example of transaction monitoring is promoted by adding deposit and withdrawal monitoring scenarios and grasping overseas transactions by detecting IP addresses.
- In light of risks associated with cash transactions, prohibiting cash transactions as a way to mitigate such risks is recognized as an example of risk assessment and an effort by business operators to implement the risk-based approach.
- An example of promoting cooperation, such as sharing necessary information and strengthening the reporting system as an initiative between the same financial group companies.

C. Assessment of Risks

There are many products in which investment is made through financial instruments business operators, etc. and commodity derivatives business operators. And it is possible to convert proceeds derived from crimes to various rights and commodities through these products.

In addition, some of these investment products involve complex schemes that can make tracking sources of invested funds difficult. Therefore, investments made through financial instruments business operators, etc. and commodity derivatives business operators can be a useful measure for ML/TF.

Indeed, there are cases where criminal proceeds from fraud or embezzlement have been invested in stocks or commodity derivatives. Considering relevant situations, it is recognized that investment made through financial

instruments business operators, etc. and commodity derivatives business operators may involve risks of misuse for ML/TF. *1 *2

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

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole. In addition, based on STRs, actual cases, etc., in addition to the transactions covered in *Section 5 High-risk Transactions*, transactions under anonymous or fictitious, borrowed names, and false names (including suspected ones) at the time of transactions and customer attributes, etc. are recognized as having an even higher degree of risk.

---

*1 Article 2, paragraph 2, item 26 of the Act on Prevention of Transfer of Criminal Proceeds provides that specified joint real estate enterprises are specified business operators. A specified joint real estate venture, which concludes a specified joint real estate venture contract (a contract stipulating that contributions will be made by the parties, of which one or more persons will be delegated to execute the business as a joint venture established with the contributions and will conduct real estate transactions, and the proceeds generated from the real estate transactions will be distributed, etc.) and distributes proceeds to investors in the course of business, can also be a way to make it difficult to track criminal proceeds. It therefore presents the risk of misuse for ML/TF.

*2 Article 2, paragraph 2, items 33 and 34 of the Act on Prevention of Transfer of Criminal Proceeds provide that book-entry transfer institutions and account management institutions are specified business operators. Book-entry transfer institutions conduct the business of book-entry transfers (and effecting pledges, etc.) of corporate bonds, stocks, etc., and account management institutions (which securities companies, banks, etc. are allowed to be) open the accounts to transfer the bonds, etc. in order to effect the book-entry transfer of company bonds etc. on behalf of another person. Products and services handled by these institutions carry risks of misuse for ML/TF.

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

A. Risk Factors

(a) Characteristics

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 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 2020, 80 business operators were engaging in trust business with such a license and authorization.

No cleared money laundering case involving misuse of trusts has been reported in Japan in recent years. However, a trust means not only to leave property with a trustee, but also has the function of changing the nominee of a property right and transferring the right to manage and dispose of the property. Furthermore, by converting property to a trust beneficiary right, the attribution, quantity and nature of the property can be altered pursuant to the purpose of the trust. From these aspects, a trust can be an effective way to conceal sources of illegal proceeds.

According to the Financial Services Agency, in transactions of trust companies, relationship with customers is not only the initial holders (consignors) and trust companies (trustees) of the above assets but also those who receive the transfer of rights to the assets(beneficiaries), forming a tripartite relationship. Furthermore, using a trust makes it possible to separate oneself from criminal proceed and conceal the relationship with criminal proceed. For which some trustees take measures according to risks of beneficiaries but each business operator takes different measures. Therefore, trust companies need to conduct risk assessment and CDD based on abovementioned characteristics.

(b) Trends of STRs

There were 50 STRs[*2] related to trusts from 2017 to 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 Boryokudan 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%)

B. 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 verification at the time of transactions against not only settlors but also 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 a right to be a beneficiary, except for some trusts.

Moreover, in addition to the supervisory measures based on the Act, the Trust Business Act and the Act on Engagement in Trust Business by a Financial Institution stipulate that the Financial Services Agency may require trust companies and financial institutions that operate trust business to report to the Agency in cases

---

*1 Trust Companies etc. mean those listed in Article 2, paragraph 2, item 24 (trust company) and item 25 (self-settled trust company) of the Act on Prevention of Transfer of Criminal Proceeds.

*2 To calculate the number, STR information was analyzed and relationships with trusts were confirmed.

where management systems for verification at the time of transactions experience some problems. Furthermore, if it is deemed that there are serious problems, the Agency 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. Specified business operators themselves are also endeavoring to establish and strengthen their AML/CFT internal control systems. For example, they are setting up a division in charge, developing internal regulations and manuals, providing periodic training, conducting internal audits, screening out transactions that are considered high-risk, and adopting enhanced monitoring for 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 system is not directly for AML/CFT purposes, but helps competent authorities to identify beneficiaries of trusts.

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

(b) Measures by competent authorities

The Financial Services Agency requires that business operators 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 Financial Services Agency conducts documentary research and issues report submission orders, and uses gap analysis, etc. to perform risk assessments on the types of businesses or operators based on the Guidelines mentioned above, and provides guidance or supervision, etc. corresponding to the risks of operators based on the assessment results.

Furthermore, in cooperation with industry associations and the Finance Bureau, the Financial Services Agency continuously provides lectures and training to financial institutions to improve money laundering measures. In 2019, 85 lectures and training were given, including those to other types of businesses. They are 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 continuous customer due diligence.

The following matters are those identified by the competent authorities that business operators should note:

- When analyzing risks, comprehensively and concretely analyze the risks, including analyzing STRs and reflecting them in document 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.
- It is necessary to secure staff with expertise and suitability through recruitment and training in the sales department, management department, and audit department.

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

(c) Measures by industry associations and business operator

The Trust Companies Association of Japan supports AML/CFT measures taken by each business operator by providing training and a range of information from external consulting companies through business communication meetings and study-group meetings on money laundering. The Association explains to each operator the details to be described and points for verification in the document prepared by specified business operators according to the intention of the respective member company, and shares opinions about establishing systems for AML/CFT measures.

Each business operator is also trying to establish and strengthen the internal control system. For example, in implementing measures against money laundering, they create documents prepared by specified business

operators, prepare rules and manuals, identify transactions that are considered high-risk transactions, and monitor high-risk transactions.

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

- Cases where risk assessment is performed for each customer considering the products, services, transaction types, countries, regions, and customer attributes and measures are taken according to the assessment.
- Cases of continuous checks on business partners' relationship with antisocial forces and records on economic sanctions, where business operators implement customer due diligence according to the trustors and trustees' risks, considering that valid right holders and their objects may become opaque due to the trust relationship.

C. 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 operators are taking, statutory measures as a matter of course, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts differs from one operator to the next, and operators taking ineffective mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and could affect the risk for the business category 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 when it comes to money lending, those who obtained criminal proceeds can make it difficult to track criminal proceeds by misusing money lending, such as by repeating debt and repayment.

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 2020, there were 1,647 registered business operators, while the outstanding balance of loans was 25.2163 trillion yen at the end of March 2019.

(b) Trends of STRs

The number of STRs submitted by money lenders, etc. was 37,224 between 2017 and 2019.

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 other person's name (18,795 reports, 50.5%)
- Transactions related to Boryokudan or their related parties (6,332 reports, 17.0%)

(c) Typologies

The following case is an example where proceeds derived from crimes were transformed:

- Case where the proceeds derived from armed robbery and fraud were spent on repayment to 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 the person and applied for a loan contract with a money lender on the Internet, and the loan was transferred to the same account.

B. 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. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the

---

*1 Money Lenders, etc. mean those listed in Article 2, paragraph 2, item 28 (money lender) and item 29 (short-term credit broker) of the Act on Prevention of Transfer of Criminal Proceeds.

transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

In addition to the supervisory measures based on the Act, the Money Lending Business Act stipulates that the competent authorities can conduct on-site inspection of, require submission of reports from or issue business improvement orders to money lenders. Comprehensive Guidelines for Supervision of Money Lenders set out points to consider when 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 that business operators 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 Financial Services Agency conducts documentary research and issues report submission orders, and uses gap analysis, etc. to perform risk assessments on the types of businesses or operators based on the Guidelines mentioned above, and provides guidance or supervision, etc. corresponding to the risks of operators based on the assessment results.

Furthermore, the Financial Services Agency cooperates with industry associations and the Finance Bureau and continuously provides lectures and training to financial institutions to improve measures against money laundering. In 2019, 85 lectures and training were given, including those to other types of businesses. They are 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 customer due diligence.

Matters to be noted by businesses that competent authorities have identified include the case examples specified below.

- In creating and reviewing documents prepared by specified business operators, they should quote the contents of national risk assessments and widely used templates. Not only that, but they should also consider the characteristics of their companies' transactions such as products, services, transaction forms, countries, and regions related to transactions, customer attributes, etc. and comprehensively 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 by giving guidance to businesses.

(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 business operator is also trying to establish and strengthen the internal control system. For example, in implementing measures against money laundering, they create documents prepared by specified business operators, prepare rules and manuals, identify transactions that are considered high-risk transactions, and monitor high-risk transactions.

The following are recognized as examples of efforts to implement the risk-based approach taken by business operators

- Cases of checking phone numbers noticed by customers with a business operator's database to ascertain that the customers' telephone numbers are unique.
- Cases of detecting suspicious and unnatural transactions by utilizing IT vendors' systems and grasping when the telephone numbers notified by the customers were used.

C. 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 a loan fraud is carried out under a fictitious name and fraudulent money is deposited into a fictitious name account that has been opened in advance. There is a risk of generating criminal proceeds.

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

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole.

In addition, based on STRs, actual cases, etc., it is recognized that transactions that involve the following transaction conditions, customer attributes, etc. are likely to present a greater risk besides the transactions covered in *Section 5 High-risk Transactions*, transactions under anonymous or fictitious names, borrowed names, and false names (including suspected ones).

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

A. Risk Factors

(a) Characteristics

A fund transfer service means an exchange transaction service (limited to transactions in which the amount is not more than 1 million yen per remittance) 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 2020, there were 75 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 11).

There are three main remittance methods in funds transfer services. One is that a client requests a fund transfer by bringing cash to a sales office of a funds transfer service provider and a receiver receives cash at another of the provider's business locations. Another is that funds are transferred between a client's account opened at a funds transfer service provider and a receiver's account opened on the website, etc. of the funds transfer service provider. The other is that 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 a card holder or a person who holds the instrument.

Fund 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. As the methods for payment, etc., cash or a money order can be received, and a deposit can be made into a bank account, etc. Various business models are being developed, and the location of risk differs for each business operators depending on the various services that each business operator is developing. For example, one business operator has constructed a system that allows it to transfer funds internationally without using the remittance network of deposit-taking institutions, developing services based on its own unique method of funds transfer.

Fund 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 the transfer of criminal proceeds to foreign countries where legal or transaction systems are different from Japan's and the traceability of the criminal proceeds decreases.

The Financial Services Agency recognizes that the risks faced by fund transfer services are limited by restrictions on the amount of money transacted. However, it is recognized that there are risk factors common to foreign exchange transactions of deposit-taking financial institutions. Under the above recognition, the Financial Services Agency requests the business operators to improve their systems. According to the Financial Services Agency, many fund transfer services providers do not comprehensively or concretely identify and assess their risks. They perform formal confirmation in verification at the time of transactions with no customer risk assessment or CDD. There are deficiencies as they do not implement management or establish a system suitable for the 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 to appropriately grasp the risks and take necessary measures to mitigate risks.

Table 11 [Trends in Fund Transfer Service Business (2017–2019)]

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) Trends of STRs

The number of STRs submitted by fund transfer service providers was 6,586 between 2017 and 2019.

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 using accounts that frequently make remittances to many persons. In particular, cases where a large amount of money was received just before remittances were made (904 report, 13.7%)
- Frequent remittances to other countries in a short period, with large amounts of remittances (581 cases, 8.8%)
- 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 (480 reports, 7.3%)
- Transactions having unnatural characteristics or conducted at an unnatural frequency considering the purpose of the transactions, occupation or business of the client, etc. (465 reports, 7.1%)
- Transactions related to Boryokudan or their related parties (445 reports, 6.8%)

On top of that, funds transfer service providers made some STRs about Money Mules[*1] in recent years. In the STRs, typically, a fund 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) Typologies

With the introduction of fund 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 examples:

- Cases including a case of Money Mule, where a person was asked to remit money overseas for a reward, and the person carried out the remittance through a fund transfer services provider while knowing that there was no justifiable reason for making the remittance
- Case where a dangerous drugs trafficker concealed his proceeds in an account opened in other person's name, then remitted the money overseas through a fund transfer services provider in order to buy material to produce the drug

---

*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.

- Case where a person, who operated an underground banking regarding oversea remittances, restocked funds that had to be pooled in the remittee country through a fund transfer services provider
- Case where an offender transferred cash derived from the sale of cars obtained through fraud to a foreign country using a fund transfer service provider
- Case where an offender had buyers, who bought fake brand goods, transfer money for purchase using a fund transfer service provider remit payment to an account under the name of the offender's relative
- Case where an illegal alien who had visited Japan as a technical intern used a funds transfer service provider to remit proceeds obtained from selling stolen goods to the leader of a foreign crime organization
- Case where a foreign crime organization made the victim remit the damages from a fraud case carried out by the organizations to a bank account in Japan, and then remitted it to the organizations by using a funds transfer service provider

and so on. 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. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires Fund 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. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

Moreover, in addition to the supervisory measures based on the Act, 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 verification 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 operator, these points are also included in the examination items related to establishing a system that is necessary for the proper and secure provision/conducting of funds transfer services. It is through these measures that the competent authorities provide AML/CFT guidance and supervision.

(b) Measures by competent authorities

The Financial Services Agency requires that business operators 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 Financial Services Agency conducts documentary research and issues report submission orders, and uses gap analysis, etc. to perform risk assessments on the types of businesses or operators based on the Guidelines mentioned above, and provides guidance or supervision, etc. corresponding to the risks of operators 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.

Furthermore, in cooperation with industry associations and the Finance Bureau, the Financial Services Agency continuously provides lectures and trainings to financial institutions to improve AML/CFT measures. In 2019, 85 lectures and trainings were given, including those to other types of businesses. They are 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.

The following matters are those identified by the competent authorities that business operators should note:

- When a funds transfer services provider whose business models, etc. are diverse analyzes risks unique to itself according to the document prepared by specified business operators, it should do so in a comprehensive and specific manner as well.
- A system for verification at the time of transaction and ongoing CDD must be established according to the risk.
- Allocating sufficient personnel in departments in charge of AML/CFT measures and thereby securing personnel with the necessary expertise and ability.
- Establish an appropriate system to examine and manage agents and implement monitoring and training regularly and 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 spoofing, at the time of opening their account.

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

(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.

Business operators themselves are endeavoring to establish and reinforce their own AML/CFT internal control systems, too. For example, they have prepared the document prepared by specified business operators, established rules and manuals, and screen out transactions that are likely to have higher risks, and adopt enhanced monitoring for transactions with higher risks.

Business scheme of funds transfer service providers vary. Some of them, for example, who 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 who deal with only refunds the return of goods or cancelled contracts, and provide limited services. Furthermore, although the scale of operators 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 operators whose efforts are insufficient.

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

- Cases where risk is evaluated for each customer by taking into account the customer attributes and transaction conditions, and measures are taken according to the assessment
- Cases of identifying and evaluating risks for services provided by a business operator acting as issuers of cards using the pre-paid payment methods when fund transfer services operate an issuer of that as a side business.
- 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

C. Assessment of Risks

Considering characteristics of foreign exchange transaction business and the fact that some funds transfer service providers provide services to remit to many countries, funds transfer services can be a useful measure for ML/TF.

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 ID to pretend to be the person. 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 indicates that the degree of risk that funds transfer services present in terms of misuse for money laundering, etc. is growing relative 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 operators are taking, statutory measures as a matter of course, the above-mentioned risk-mitigating measures.

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole.

In addition, based on STRs, actual cases, etc., it is recognized that transactions that involve the following transaction conditions, customer attributes, etc. are likely to present a higher risk, besides the transactions specified in *5 High-risk Transactions* in this survey, the following items are recognized as having an even higher risk regarding the situation at the time of transaction and the attributes of customers.

- 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[*1] such as Bitcoin have proprietary value (limited to that which is recorded on electronic equipment by an electronic method and which excludes currency and assets in currency) that can be used to pay unspecified persons, when purchasing goods, etc., for the reimbursement of the price and that can be purchased from and sold to unspecified persons as counterparties. Also, they are 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 September 2020, there are 26 registered business operators.

The transaction amounts in these crypto-assets are increasing globally including Japan, and, as a result, the number of cleared cases involving crypto-assets is rising. In Japan, 22 cases of unauthorized transmission by unauthorized access, etc. to crypto-assets exchange service providers occurred in 2019, with damages of about 3.1286 billion yen. July of 2019 saw cases where huge amounts of crypto-assets seemed to be illicitly transmitted from domestic crypto-assets exchange service providers.

In the background behind some of these cases, there are circumstances in which appropriate internal control systems for various risks, including money laundering, could not keep up with the rapid expansion in business scale of operators handling crypto-assets.

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 them, one is known to exist for which a record of transfer will not be made public, making it difficult to trace transactions, and thus is likely to be used for money laundering. Another is known to be poor at maintaining and updating its transfer records.[*2] 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.

And since almost all transactions handled by crypto-assets exchange service providers are not conducted in person but over the Internet, they have high anonymity, relatively speaking. If crypto-assets that have been rendered even more anonymous as explained above are exchanged in transactions, subsequent tracking of those transactions is much more difficult.

With respect to the exchange of crypto-assets and legal currency, there are crypto-assets ATMs, where crypto-assets and legal currency 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. It is expected that crypto-assets exchange service providers may study the possibility of establishing crypto-assets ATMs or increasing the number of units in anticipation of the increase in demand. However, since cases are occurring overseas in which drug traffickers exchange proceeds derived from drug trafficking into crypto-assets via crypto-assets ATMs, it is necessary to watch how such ATMs are actually being used by pretending to be small amount transaction or not regular transaction.

The Financial Services Agency is requesting crypto-assets exchange service providers to establish and upgrade a risk management system and effective business operations based on a risk-based approach, in addition to complying with laws and regulations. Furthermore, the Financial Services Agency is requesting them to take measures to mitigate risks, such as verification at the time of transactions linked with customers'

---

*1 In accordance with the Act on the Partial Revision of the Payment Services Act to Support Diversifying Financial Transactions Due to Advancement of Information and Communication Technology (Act No. 28 of 2019, Act for Partial Revision of the Payment Services Act) promulgated on June 7 of 2019, "virtual currency" as stipulated in the Payment Services Act, the Act on Prevention of Transfer of Criminal Proceeds, etc. was revised to the term, "crypto-asset" (effective on May 1, 2020).

*2 Until recently, the names of crypto-assets handled by crypto-assets exchange service providers were reported after the JVCEA review so that the government could appropriately respond to them. Under the Act for Partial Revision of the Payment Services Act, such names must be reported in advance.

risk assessment. When providing a new service to improve customer convenience, it may not be possible to capture the risk of the service with conventional measures to mitigate risks. Therefore, it is necessary for business operators to correctly grasp the risks and take necessary measures to mitigate risks each time.

FATF also revised the FATF Recommendations (Recommendation 15) in October 2018 and has requested each country to impose regulations for countermeasures against ML/TF, on service providers who exchange crypto-assets with legal currency, and to introduce a licensing or registration system for such providers. As a result of this revision, the Interpretative Notes to the Recommendations and the Guidance on crypto-assets published in June 2015 were revised in June 2019 to present the concept of the risk-based approach pertaining to crypto-assets.

(b) Trends of STRs

The number of STRs submitted by crypto-assets exchange service providers during the period from April 2017 to the end of 2019 was 13,761.

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 major ones by 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 (1,694 cases, 12.3%)
- Transactions related to accounts that receive remittances of money or crypto-assets under the names that seem to be anonymous or fictitious (582 cases, 4.2%)
- Transactions related to Boryokudan or their related parties (512 cases, 3.7%)

The contents of suspected transactions under fictitious and borrowed names shown below.

- 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

and so on.

(c) Typologies

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

- Case where 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
- Case where 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

and so on.

The following examples are cases 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:

- 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.

- Case where an offender opened accounts with crypto-assets exchange service providers using the principal identification documents of another person

and so on.

Other case where crypto-assets was used as the means of payment in crimes:

- Case where crypto-assets was used for transactions of illegal drugs or for payment of special points that were necessary to download child pornography

and so on.

B. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires crypto-assets exchange service providers*1 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 concerning opening of wallets), 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. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like. Furthermore, the Act 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, a party operating a crypto-assets service must be registered by the prime minister, and the party assumes the obligation to submit business reports under the Payment Services Act. The Payment Service Act stipulates that the competent authorities may enter a crypto-assets exchange service provider's office for inspection and issue business improvement orders, etc., to crypto-assets service operators if necessary. In addition, the Act also provides the grounds for refusing or rescinding the registration of a crypto-assets exchange service provider, as a corporation that has not established a system to properly and securely conducting crypto-assets exchange service business. Moreover, the Guidelines for Administrative Processes by the Financial Services Agency set out points to consider when establishing internal control systems for verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds. When business operators apply for registration as a crypto-assets exchange service provider, these points are also included in the examination items related to establishing a system that is necessary for conducting proper and secure crypto-assets exchange service business. The competent authorities are introducing these measures into the system for guidance on AML/CFT, and actually executing them.

(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 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 6 warnings as at the end of March 2020.

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

---

*1 According to the Act for Partial Revision of the Payment Services Act, crypto-assets management services conducted as business to manage other people's crypto-assets, regardless of the exchange, etc. of the crypto-assets, have been added to the crypto-asset exchange services in the Payment Services Act, and those who are engaged in crypto-asset management services have been added to specified business operators that are subject to obligations under the Act on Prevention of Transfer of Criminal Proceeds.

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.

Furthermore, in cooperation with industry associations and the Finance Bureau, the Financial Services Agency continuously provides lectures and training to financial institutions to improve AML/CFT measures. In 2019, 85 lectures and training were given, including those to other types of businesses. They are 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.

The following matters are those identified by the competent authorities that business operators should note:

- The management must formulate effective measures to mitigate risks and promote and establishing a system while taking the initiative and proactively participate in giving specific instructions and coordinating related departments.
- The management department must establish a system that can actively implement the risk-based approach and PDCA cycle and promote compliance with laws and regulations.
- Internal auditing is not limited to rule-based auditing but must conduct a risk-based approach.
- With regard to identification and assessment of risks, comprehensive verification, which includes identification and assessment of individual risk factors such as countries/regions and products/services, must be conducted. There are some business operators who work on improving their methods by introducing a scoring system. It is still necessary to conduct comprehensive risk-based verification, such as checks on whether documents prepared by specified business operators are only limited to formal descriptions and whether risk assessments are being conducted when introducing new products and services.
- Measures to mitigate risks should not be limited to the application of legal requirements, such as verification at the time of transaction and to quoting the contents of national risk assessments and widely used templates. Regarding the results of an analysis to be compiled in a document prepared by a specified business operator, 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 competent authorities have made improvements and corrections with respect to these matters by providing instructions, etc. to business operators.

The Financial Services Agency executed administrative action of business suspension orders or business improvement orders to crypto-assets exchange service providers, etc., in the following cases:

- Case where the verification at the time of transactions and the judgment on the need for STRs were not performed in connection with the sale and purchase of a large amount of crypto-assets on more than one occasion
- Case where crypto-assets exchange services were offered without sufficiently performing verification at the time of transactions
- Case where the system to confirm the verification at the time of transactions was not in place, and employees did not receive verification training
- Case where, although the Agency had given guidance, no corrections were made since there was nobody available who sufficiently understood the details of the request for correction

For the reasons mentioned above, the Agency executed administrative actions for 29 business suspension orders and business improvement orders as at the end of March 2020.

(c) Measures by industry associations and business operator

At the initiative of 16 crypto-assets exchange service providers, a new industry association called the Japan Virtual Currency Exchange Association (currently Japan Virtual and Crypto assets Exchange Association) was founded in March 2018. It was approved by the Financial Services Agency in October of the same year. 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 recognized as examples of efforts to implement the risk-based approach taken by business operators:

- For those related to risk identification and assessment
  - Cases where 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.
  - Cases where a business operator comprehensively identifies and evaluates its own services, in addition to the exchange, etc. of crypto-assets.
  - Cases where not only risks directly related to ML/TF, but also other risks that may have indirect impact such as hacking risk, are evaluated.
  - Cases where a business operator identifies and assesses risks for each type of crypto-assets it handles, focusing on bad reputation, liquidity, etc.
- For those related to the risk-based approach
  - Cases where 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.
  - Cases where 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.
  - Cases where as of the risk of using services in process of specialized fraud, the results of investigation and analysis related to the unnatural matching of customers' characteristics, such as their photos on identity verification documents and customer attributes found in the verification at the time of transactions, are reflected in documents prepared by specified business operators and verification at the time of transactions is strengthened.
  - Cases of strengthening the monitoring of transactions with countries judged to be highly risky and customers in the same countries by focusing on prosecution cases and media reports on financial crime-related remittances, risk analyses and the corruption perception indexes (CPIs) conducted by other countries' authorities.
  - Cases where the period of stay of foreign customers, such as international students and workers, is managed by a system after confirming it to deal with risks such as the sale of accounts at the time of their return to their home countries.

C. Assessment of Risks

Important characteristics of crypto-assets are that its users are highly anonymous and that the transfer of crypto-assets can be quickly executed across national borders. In addition, regulation of crypto-assets differs from country to country. In light of these factors, if crypto-assets are misused for crimes, it becomes difficult to trace the proceeds derived from the crimes.

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 have the money remitted to an

account opened in another person's name, it is recognized that crypto-assets is at risk of being misused for ML/TF. In addition to the transactions covered in *Section 5 High-risk Transactions*, transactions under anonymous or fictitious names, borrowed names, and pseudonyms (including suspected ones) at the time of transactions and customer attributes, etc. are recognized as having an even higher degree of risk.

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.

Against such risks, competent authorities and industry associations are executing the statutory measures as a matter of course, risk-mitigating measures as above mentioned. The effect of these risk-mitigating measures is that the number of STRs by operators appear to be rising substantially, and that operators who fail to take appropriate action against money laundering receive business suspension orders, forcing them to suspend their services.

However, it is not easy to take appropriate and timely risk-mitigating measures amid rapid changes in the environment surrounding crypto-assets transactions, and if such these efforts are insufficient, appropriate mitigating measures cannot be taken and the degree of risk will remain high.

(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 12).

By physically taking criminal proceeds overseas, it is possible to lower the possibility of detection of the proceeds, punishment, confiscation, etc. Furthermore, if criminal proceeds are exchanged into foreign currency and moved across borders, it is also possible to use the proceeds while reducing the probability of arrest, confiscation and other punishments. Furthermore, foreign-currency exchange has the characteristics of handling cash, which is high in liquidity and anonymity, and the capability of physically changing the form of criminal proceeds and exchanging a large number of small-denomination bills for a smaller number of large-denomination bills. In addition, non-face-to-face transactions are possible 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 12 [Transactions by Foreign Currency Exchange Operators (2017 - 2019)]

Reporters		2017				2018				2019			
		Number of reporters	Number of transactions	Transaction value (million yen)	Value per transaction (1,000 yen)	Number of reporters	Number of transactions	Transaction value (million yen)	Value per transaction (1,000 yen)	Number of reporters	Number of transactions	Transaction value (million yen)	Value per transaction (1,000 yen)
Deposit-taking institutions	Major banks (Note 2)	4	280,019	21,230	76,244	4	224,970	25,462	116,737	4	181,410	26,326	145,738
	Regional banks	94	188,135	12,341	65,862	92	185,578	11,969	64,613	88	183,687	10,554	57,653
	Shinkin banks	126	4,619	463	100,477	120	4,222	398	95,023	110	3,716	326	88,446
	Foreign banks	26	2,967	5,331	4,544,074	26	660	2,612	3,051,127	24	375	124	328,477
	Other deposit-taking institutions (Note 3)	9	36,105	2,184	61,727	9	79,290	4,394	56,074	9	101,683	5,008	49,344
Excluding deposit-taking institutions	Funds transfer service/credit card business	13	182,483	9,976	54,698	14	202,066	12,707	62,622	15	230,404	14,952	65,065
	Hoteliers	50	4,888	640	108,558	42	3,538	393	91,286	34	2,813	161	58,883
	Travel agencies	31	61,921	2,984	49,070	28	60,734	2,745	46,016	26	54,899	2,421	45,937
	Secondhand dealers	50	55,805	4,096	73,739	46	54,809	4,005	73,368	48	49,297	3,701	75,139
	Service providers related to airports	5	140,318	4,757	33,959	5	153,773	5,099	33,161	6	154,056	5,377	35,283
	Large-scale retailers	3	429	11	25,277	3	344	9	24,928	2	230	6	25,949
	Others	61	63,991	8,872	136,159	126	90,680	15,586	168,613	64	109,611	34,756	355,879
	Total	472	1,021,680	72,885	71,338	515	1,060,664	85,379	80,496	430	1,072,181	103,712	96,730

Note 1: Based on 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 value per transaction is large because some banks procure/buy foreign currency with other financial institutions.
4: The Shinkin Central Bank, credit associations, Japan Post Bank, and other banks.

(b) Trends of STRs

The number of STRs submitted by foreign-currency exchange operators between 2017 and 2019 was 1,851.

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 (607 reports, 32.8%)
- Frequent buying and selling of foreign currency or traveler's checks in a short period of time (170 reports, 9.2%)
- When counterfeit currency, stolen currency, or suspected currency is received (75 cases, 4.1%)

(c) Typologies

The following is an example case of misuse of foreign-currency exchange for money laundering in Japan:

- Case where a large amount of foreign currency obtained due to robbery and murder overseas was converted to Japanese yen through a third party

Meanwhile, the following case is an example from abroad:

- Case where a drug-trafficking organization used unregistered foreign-currency exchange operators to convert drug proceeds to foreign currency

and so on. Meanwhile, the following case is an example where criminal proceeds were transformed.

- Case where foreign-currency funds obtained in a robbery case in Japan were converted into Japanese yen

and so on.

B. Measures to Mitigate Risks

(a) Statutory measures

Many of the foreign-currency exchange operators are subject to business regulations related to their main business, i.e., their obligation to obtain a business license, competent authorities' supervision, etc. In addition, 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. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

Moreover, in addition to the supervisory measures based on the Act, 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 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.

And, based on the results of on-site inspections and documentary research on compliance with laws and regulations and of risk control, the Ministry is performing risk assessments on respective operators from the perspectives of the scale of currency-exchange transactions, internal control systems, the existence of non-face-to-face transactions and, based on the results, providing guidance and supervision corresponding to the risks.

Consequently, it has been found that there are many business operators who do not analyze their own transaction risks, as they do not prepare the document prepared by specified business operators or they cite a standard template as it is. For such business operators, the Ministry provides guidance during an on-site inspection so they will identify and assess their transaction risks. For business 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 form, whether substantive risk mitigation measures have been taken in accordance with the Foreign Exchange Inspection Guidelines based on the abovementioned assessment. If the Ministry detects inadequate implementation, it will provide guidance for the business operator.

Furthermore, the Ministry holds briefing sessions on obligations, etc. under the Act on Prevention of Transfer of Criminal Proceeds for foreign-currency exchange operators. In 2019, the Ministry of Finance attended six briefings held by the Japan Ticket Association, Japan Association of Travel Agents, Japan Department Stores Association, and Japan Exchangers Safety Council to explain the obligations under the Act on Prevention of Transfer of Criminal Proceeds in Money Change Business. 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 obligations and supervision are important for grasping the actual state of foreign-currency exchange and to prevent foreign-currency exchange from being misused for ML/TF.

The following matters are those identified by the competent authorities that business operators should note:

- Management needs to play a leadership role with respect to AML/CFT measures.
- 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.
- Appoint a manager (manager of verification at the time of transaction) responsible for the performance of verification at the time of transaction.
- 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.
- Training must be provided to employees who are engaged in counter services.
- The supervisor must correctly understand his obligations under the Act on Prevention of Transfer of Criminal Proceeds, even in small-scale 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 so that no vulnerabilities exist in the entire internal control system pertaining to AML/CFT measures.
- 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.
- When preparing a written Risk Report Assessment by a Specified Business Operator, 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.
- Verifying the client identity, the purpose of transaction, beneficial owner, etc.
- 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.
- Creating and saving verification records.
- 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 STR(s).

- 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 business 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 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, operators who handle lower volumes tend to be modest in taking such measures.

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

- Cases where 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 are specified in internal regulations.
- Cases where, 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.
- Cases where 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.
- Cases where suspicious transactions are examined in order to submit STR(s) 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.
- Cases where 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.
- Cases where 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.

C. 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 operators are taking, statutory measures as a matter of course, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole.

In addition, based on STRs, actual cases, etc., it is recognized that transactions that involve the following transaction conditions, customer attributes, etc., besides the transactions specified in 5. High-risk Transactions in this survey, the following items are recognized as having an even higher risk regarding the situation at the time of transaction and the attributes of customers.

- 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. In that case, a person associated with Boryokudan received goods through financial leasing and allowed a head of the Boryokudan to use them for a long time.

(b) Trends of STRs

The number of STRs submitted by financial leasing operators between 2017 and 2019 was 601. 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 or their related parties (258 reports, 42.9%)
- 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”) (121 reports, 20.1%)
- 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”) (62 reports, 10.3%)

B. 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 requires business operators to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like. Moreover, 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 business 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 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. In addition, the Japan Leasing Association undertakes documentary research on members of the Association every year and executes the risk assessment for ML/TF, based on the results, etc., of such research, and checks the beneficial owners of its 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.

Respective business operators also establish basic policies and response manuals for AML/CFT measures, 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.

C. 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 operators are taking, statutory measures as a matter of course, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole.

In addition, based on STRs etc., it is recognized that transactions that involve the following transaction conditions, customer attributes, etc., besides the transactions specified in *5. High-risk Transactions* in this survey, the following items are recognized as having an even higher risk regarding the situation at the time of transaction and the attributes of customers.

- 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, 2020, 255 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) Trends of STRs

The number of STRs submitted by credit card operators was 55,253 between 2017 and 2019.

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 (15,048 reports, 27.2%)
- Cases in which it was suspected that a person who was not a true card holder uses the credit card (11,091 reports, 20.1%)
- Transactions related to Boryokudan or their related parties (10,417 reports, 18.9%)

(c) Typologies

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

- A case where 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 case where 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 case where a shop owner operating a loansharking business executed 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

and so on.

---

*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).

B. 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. The Act also requires them to file STRs when received property is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

In addition to the supervisory measures based on the Act, 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 business operators are requested to establish and maintain risk management systems for ML/TF based on the Guidelines, and 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 business operators.

The following matters are those identified by the competent authorities that business operators should note:

- 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,

and so on. The competent authorities have made improvements and corrections with respect to these matters by providing instructions, etc. to business 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 business operator by instilling members' understanding of measures, including those against money laundering. In accordance with the registration/inquiry system, etc. on credit card member information by credit information institutions designated by the Minister of Economy, Trade and Industry under the Installment Sales Act, the Association also checks for the presence of any suspicious points such as a large number of applications for credit cards made in a short period, so that business operators can use the results as references when deciding whether to conclude, renew, etc. contracts.

Business 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 to implement the risk-based approach taken by business operators:

- Cases where 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
- Cases where 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 money laundering using a contracted card

C. 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 operators are taking, statutory measures as a matter of course, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole.

In addition, based on STRs, actual cases, etc., besides the transactions specified in *5. High-risk Transactions* in this survey, the following items are recognized as having an even higher risk regarding the situation at the time of transaction and the attributes of customers.

- 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 125,638 brokers as of the end of March 2020. In 2018, the annual amount of sales were about 47 trillion yen, and in 2018 the annual number of transactions that were registered and notified to the real estate 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) Trends of STRs

The number of STRs submitted by real estate brokers was 21 between 2017 and 2019. 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 (8 reports, 38.1%)
- Unusual transactions or transactions related to customers who show unusual behavior or actions, based on the knowledge and experience of their own employees (5 reports, 23.8%)

It can be said that the number of STRs is small compared to the business scale. However, some of STRs were made from the following points of view. This information is considered useful for the entire business operators.

- STR of transactions where a large amount of cash was paid, which was not appropriate for the customers' ages, occupations, etc.
- STR about suspicions of the source of funds, such as those about customers who show an attitude of sticking to cash transactions as a 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) Typologies

The following cases is an example of misusing real estate for money laundering in Japan:

- A case where the proceeds derived from prostitution were used to purchase land in a relative's name

Meanwhile, the following case is an example from abroad:

- A case where drug traffickers bought real estate with drug proceeds in their friend's name, and used the real estate for living and drug manufacturing

and so on. Meanwhile, the following case is an example where criminal proceeds were transformed.

- A case where proceeds from fraud were used to buy a condominium

and so on.

B. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires real estate brokers to conduct verification at the time of transactions and prepare and preserve verification records and transaction records when they make a purchase and sale contract for building lots and buildings, or conduct intermediary or agency service thereof. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

Furthermore, in addition to the supervisory measures based on the Act, 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. 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 performs documentary research or hearings to grasp the actual status of compliance with legal regulations and risk control by business operators, and provides guidance and oversight, etc., corresponding to risks of respective business operators based on information obtained through such research and orders. In addition, the Ministry has established an industry-wide liaison council of six real estate trading organizations as well as and also Real Estate Business and Police Central Liaison Committee for Exclusion of Boryokudan, etc., aiming to enhance the collaboration between related administrative organs and the real estate industry, and to promote the elimination of anti-social forces such as Boryokudan from real estate transactions, and information is exchanged with these councils.

Furthermore, each Regional Development Bureau and prefecture conducts an annual on-site inspection on real estate brokers to check the status of the creation of confirmation records and transaction records based on the Act on Prevention of Transfer of Criminal Proceeds. In September of 2019, the Ministry of Land, Infrastructure, Transport and Tourism held a workshop on residential land and building transaction sponsored by Osaka Prefecture and by the Aichi Prefecture Housing Construction Association, regarding AML/CFT measures and explained high-risk transactions.

The following matters are those identified by the competent authorities that business operators should note:

- 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 businesses.

(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 business operators' 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 business operators:

- Cases where information on transactions with customers for whom transactions were cancelled or transactions were not performed for any reason in the past placed into a database for employees in the company to share and, if any subsequent transactions with such customers occur, measures are taken to enhanced customer due diligence or to reject those transactions
- A case where, in order not to overlook transactions with Anti-social Forces, an operator independently prepares a checklist on the characteristics of speech and behavior of anti-social forces and utilizes the checklist for customer due diligence

C. 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, etc. 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 operators are taking, statutory measures as a matter of course, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole.

In addition, based on STRs, actual cases, etc., it is recognized that the transactions covered in *Section 5 High-risk Transactions*, transactions under anonymous or fictitious names, borrowed names, and pseudonyms (including suspected ones) are likely to present a higher risk.

(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 value, and they can be easily exchanged for cash anywhere in the world. Other than that, they are small, so are easy to carry, and it is difficult to track distribution channels and locations after transactions. Transactions related to precious metals and stones have high anonymity.

In cases where a person imports or exports by carrying precious metals[*1] weighing more than 1 kg hey are required to make a prior declaration to Customs under the Foreign Exchange Act and the Customs Act (Act No. 61 of 1954). However, in recent years, smuggling of gold bullion has been growing. In administrative year[*2] 2018, the number of processed cases (notifications and indictments) of gold smuggling was 404 and the value of evaded tax was approximately 960 million yen, which was the second highest in history after the record high in fiscal 2017 (see Tables 13 and 14). Although the number of gold bullion smuggling cases in fiscal 2018 decreased significantly, the number of disposals was still high because the results of the cases caught before fiscal 2017 were included.

A method recently seen in gold smuggling cases is an attempt to obtain illicit profit using differences between tax systems; specifically, the method of deception is to purchase gold bullion in a tax-exempt country or region, smuggle it into Japan to avoid paying consumption tax, and then sell it at jewelry stores, etc. in Japan at the price that includes consumption tax to obtain a profit equivalent to consumption tax. Also, smuggling methods have become more sophisticated such as processing the gold or changing its shape to conceal it in a body cavity or clothing, etc. and miniaturized, such as repeatedly smuggling a large quantity of gold concealed in automobile parts. Likewise, there has been a trend in the diversification of smuggling methods such as using airline passengers, air cargo, and international postal mail, etc., and dispersing entrance via air to smaller local airports, and so on. Hong Kong and Korea are the major sources of smuggled shipments. In addition, a circular scheme to repeat the acquisition of criminal proceeds has been observed in which gold bullion purchased abroad from criminal proceeds obtained by the above-mentioned smuggling is smuggled into Japan again and sold in retail shops in Japan. There is background recognition of the actual situation involving domestic and overseas organizations, such as Korean illicit dealers, Boryokudan-related persons, and so on.

Furthermore, gold bullion prices are liable to fluctuate and cash payment is the main transaction arrangement, which is one of the reasons why gold transactions are highly anonymous.

According to the Ministry of Economy, Trade and Industry, when jewelry dealers trade jewelry, they often pay by credit card or bank transfer, and cash transactions are few. Therefore, the risk of abuse for ML/TF is evaluated as 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 of a scale unsuitable for the company size or transactions with non-residents, have a high risk of abuse 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 2018 to June 2019.

Table 13 [Changes in the Number of Cleared Cases of Gold Bullion Smuggling (Administrative Year 2016–2018)]

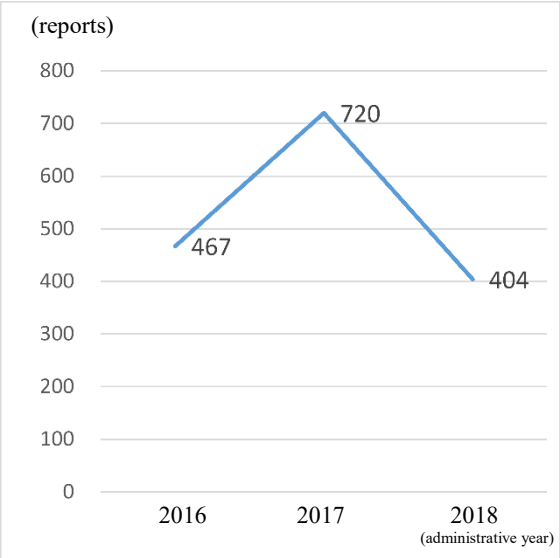
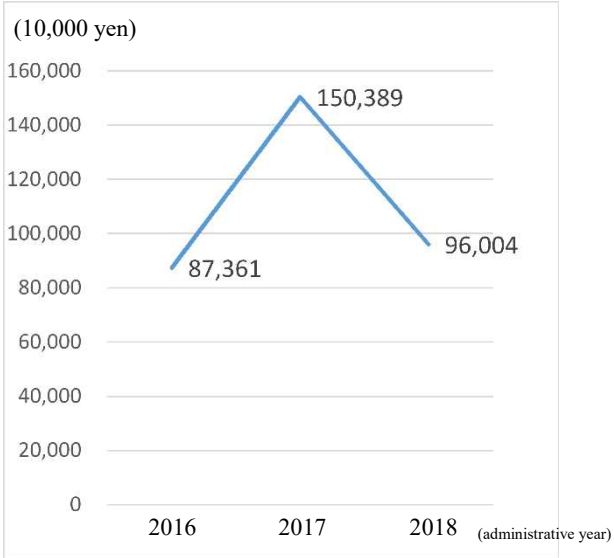


Table 14 [Changes in the Amount of Evaded Taxes in the Cases of Gold Bullion Smuggling (Administrative Year 2016–2018)]



(b) Trends of STRs

The number of STRs submitted by dealers in precious metals and stones was 1,315 between 2017 and 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.

- The same person/company buying and selling a large amount of precious metals in a short period (795 reports, 60.5%)
- Purchases using large amounts of cash (120 reports, 9.1%)
- Unusual transactions or transactions related to customers who show unusual behavior or movements, based on the knowledge and experience of their own employees (115 reports, 8.7%)

(c) Typologies

The following cases are examples of misusing precious metals and stones for money laundering in Japan.

- A case where an offender made an acquaintance sell gold bullion obtained through theft in the name of a judicial person
- A case where precious metals were purchased in the name of another person at a jewelry store using cash obtained through theft

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 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. 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. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are

suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

In addition to the supervisory measures based on the Act, the Secondhand Articles Dealer Act (Act No. 108 of 1949) and the Pawnbroker Business Act (Act No. 158 of 1950) provide that police staff, etc., may conduct on-site inspection of and issue business suspension orders to secondhand articles dealers and pawnbrokers if 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 concerned ministries and agencies, such as amendments to relevant laws and regulations. This includes requiring the complete fulfillment of obligations for business operators who are involved in the logistics of gold bullion, under the Act on Prevention of Transfer of Criminal Proceeds, to secure 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 operators, and provides the guidance and supervision, etc., corresponding to risks faced by certain business operators based on information obtained through such research. Specifically, since the actual search revealed more than one gold bullion dealer who failed to notify the administrative authority of the existence of a customer who repeatedly conducted suspicious transactions to purchase a large amount of gold bullion in cash during a short period, the Ministry provided administrative guidance to these operators in April 2018 and 2019, the content of which was as follows:

- To report suspicious transactions promptly
- To prevent violations from recurring, take measures to further strengthen education and training for employees and to fulfil the obligations to verify transactions, including by establishing and reviewing regulations

and so on.

In addition, the Ministry is working to provide administrative guidance, such as by issuing guidance documents to operators who are considered to have insufficient understanding of risk control, etc., and by holding seminars for the industry. Furthermore, the Ministry's website has a page for receiving questions about the Act, and is accepting inquiries from business operators to ensure they fulfil their obligations.

At a briefing session for jewelry handling business operators held in January 2019 by the Ministry of Economy, Trade and Industry and the Japan Jewelry Association, Ministry officials with National Police Agency officials explained the matters to be observed based on the Act on Prevention of Transfer of Criminal Proceeds. Furthermore, at a workshop for the member companies of the Japan Gold Metal Association in November 2019, Ministry officials with Ministry of Finance officials explained the matters to be observed based on the Act on Prevention of Transfer of Criminal Proceeds. The following matters are those identified by the competent authorities that business operators should note:

- 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

(c) Measures by industry organization and business operator

To preventing 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 is also working to communicate the Act on Prevention of Transfer of Criminal Proceeds to all its members by distributing posters, etc. targeted specifically to them, holding training sessions, and publicizing the information on its website, etc.

The Japan Jewelry Association is working to improve the level of understanding of business operators, etc. about money laundering, etc. by distributing leaflets and booklets that give an overview of the Act on Prevention of Transfer of Criminal Proceeds and the details of obligations that business operators must fulfil,

holding briefing sessions on AML/CFT measures, and updating websites, etc. to communicate the information.

To promote initiatives for preventing ML/TF, industry organizations related to secondhand article dealings are communicating AML/CFT measures to all business operators by creating manuals summarizing the manner of performing obligations under the related laws (Act on Prevention of Transfer of Criminal Proceeds and Secondhand Articles Dealer Act) and holding training sessions. In addition, 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. Furthermore, operators 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.

C. Assessment of Risks

Precious metals and stones have high value and are distributed all over the world. It is easy to exchange them for cash or carry them around. In addition, the difficulty of tracking their distribution channels and locations after purchase and sale gives them high anonymity. In particular, gold bullion transactions are mainly conducted through cash payment, meaning anonymity may become even higher. Therefore, precious metals and stones can be an effective instrument for laundering money.

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 money laundering is increasing.

Against such risks, competent authorities and operators are executing statutory measures as a matter of course, risk-mitigating measures as above mentioned. As a result, these risk-mitigating measures appear to be seeing some success as shown by the fact that recognition by business operators is improving and the number of STRs has substantially increased.

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole.

In addition, based on STRs, actual cases, and the like, besides the transactions specified in *5. High-risk Transactions* in this survey, the following items are recognized as having an even higher risk regarding the situation at the time of transaction and the attributes of customers.

- 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 such a 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.

During investigations related to specialized fraud, etc., from 2017 through 2019, the National Public Safety Commission collected reports on 7cases based on the Act on Prevention of Transfer of Criminal Proceeds from postal receiving service. Specific cases of violation identified through the submitted reports are as follows:

- Neglected to verify the purpose of customers' transactions, their occupations, etc.
- Neglected to verify the beneficial owner of corporate customers
- Neglected to send transaction-related documents by registered mail that must not be forwarded or the like in non-face-to-face transactions
- Neglected to prepare or keep verification records

and so on.

The Ministry of Economy, Trade and Industry has assessed that business operators who accept non-face-to-face contract applications and who allow customers to use the operators' own addresses for legal person's registration are at high risk of being misused for ML/TF.

(b) Trends of STRs

The number of STRs from postal receiving service providers between 2017 and 2019 was 12.

The Ministry of Economy, Trade and Industry revised and published in April 2017 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 (3 reports, 25.0%). When applicants were inquired about basic matters, such as their age, they could not answer. Accordingly, STRs were submitted. There were also STRs about cases where others impersonated contractors and came to pick up parcels.

(c) Typologies

The following cases are examples of misusing postal receiving services for money laundering:

- Cases where proceeds derived from specialized fraud were forwarded to several locations, including a postal receiving service provider, and then received by the offender
- Cases where loan repayments in underground banking and proceeds derived from selling obscene DVDs were sent to postal receiving service providers with which contracts were concluded in other persons' names

and so on.

B. 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 also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like. Furthermore, the Act provides for supervisory measures by the competent authorities, such as requiring the submission of reports and conducting an on-site inspection.

(b) Measures by competent authorities

In order to ensure thorough compliance by postal receiving service providers, the Ministry of Economy, Trade and Industry holds briefing sessions for them and outlines the Act on Prevention of Transfer of Criminal Proceeds and important points of their obligations under the Act, and distributes documents to postal receiving service providers to raise awareness about matters to be verified at the time of transaction. In addition, the Ministry sends brochures to inform postal receiving service providers of verification at the time of transactions. It also explains the Act on its website.

Furthermore, the Ministry summarized the actual conditions and issues of postal receiving service providers industry and the risk of misuse for crimes. Simultaneously, the Ministry formulated and published guidance for postal receiving service providers to introduce examples of efforts to prevent misuse for crime. 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 conducts on-site inspections, issues rectification orders and provides guidance based on the Act on Prevention of Transfer of Criminal Proceeds to providers who violated the obligation of verification at the time of transaction, and raises awareness of the performance obligations based on the Act. It issued two rectification orders to postal receiving service providers during the period from 2017 to 2019, the contents of which are as follows:

- To implement internal regulation in order to improve in-house training at companies on the Act on Prevention of Transfer of Criminal Proceeds and to devise in-house rules to facilitate administrative procedures related to the Act
- To review work related to verification at the time of transaction and to prepare and retain verification records

and so on.

In addition, the Ministry undertakes documentary research and surveys to grasp the actual state of compliance with laws and regulations and of risk management by business operators. It also provides guidance and supervision, etc., relating to risks faced by respective business operators based on information obtained through such research and surveys, as well as from verification results relating to violations, etc.

The following matters are those identified by the competent authorities that business operators should note:

- Establishing internal regulations, manuals, etc. for compliance with laws.
- Verifying the client’s identity, the purpose of transaction, beneficiary owner, etc.
- Creating and saving 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,

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

(c) Measures by business operators

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

- Cases where information on customers with whom transactions were cancelled or could not be achieved in the past for any reason is shared among other companies in the same industry to strengthen customer control
- Cases where suspicious situations are summarized, and manuals, contract examination standards, contract refusal standards, etc. to reflect such cases in business operations are established.

C. 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 business operators need to take, statutory measures as a matter of course, the abovementioned measures to mitigate these risks.

However, the level of these efforts differs from one operator to the next, and operators taking ineffective risk-mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and influence the risk for the business category as a whole.

In addition, based on STRs, actual cases, etc., besides the transactions specified in *5. High-risk Transactions* in this survey, the following items are recognized as having an even higher risk regarding the situation at the time of transaction and the attributes of customers.

- 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 business operators that conduct non-face-to-face verification at the time of transaction, and other business operators with few workers that have not established a management system, in particular are high risk of being misused for ML/TF.

(b) Trends of STRs and 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. The number of STRs from telephone receiving service providers between 2017 and 2019 was none.

B. 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 also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like. In addition, the Act 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

In order to ensure telephone receiving service providers' compliance, the Ministry of Internal Affairs and Communications holds briefing sessions for them and explains the outline of the Act on Prevention of Transfer of Criminal Proceeds and important points of their obligations under the Act. The Ministry also explains 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, the Ministry sent an overview document of the Act on Prevention of Transfer of Criminal Proceeds to telecommunications carriers that providing telephone receiving services and telephone forwarding services to disseminate information that needed to be grasped. The document also described the items to be confirmed at the time of transaction.

The Ministry also undertakes documentary research and surveys to grasp the actual state of compliance with laws and regulations as well as risk control by business operators, and based on that information, provides guidance and supervision, etc., corresponding to risks facing relevant businesses.

The following matters are those identified by the competent authorities that business operators should note:

- 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,

and so on. The competent authorities are to make improvements and corrections with respect to these matters by providing instructions, etc. to business operators.

C. Assessment of Risks

Recently we have not seen any cleared cases for money laundering involving misuse of a telephone receiving service. 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, the level of these efforts differs from one operator to the next, and business operators that are not taking effective mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and could affect the risk for the business category 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.

By using such a service, customers can announce a telephone number that is different to their home or office as their telephone number, and can receive telephone calls using the provider's number. Because of these characteristics, telephone forwarding services are misused in specialized fraud, etc. Indeed, telephone forwarding services have been misused to provide contact points used by suspects in some false billing fraud cases, where victims were fraudulently charged for the purchase of securities.

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 2020, there were 846 providers that had applied to provide telephone forwarding services.

In recent years, there have been actual cases in which telephone transfer services that can display the telephone number of a landline phone, such as a 03 number, have been misused in specialized fraud, etc. to hide from other parties the origin or destination of smartphones and other mobile phone terminals, etc., without a telephone number by going through switching equipment or a cloud PBX provided by a business operator. The method of deception is changing from misuse of rental mobile phones in the past.

Actually, the number of reports from prefectural police to the National Public Safety Commission that such services have been used for crimes including specialized fraud, etc. and that suspected violation of obligations to verify at the time of transaction has been recognized regarding telephone forwarding service providers have been increasing since 2017.

As such, the National Public Safety Commission collected 21 submission reports from 2017 through 2019 under the Act on Prevention of Transfer of Criminal Proceeds. Specific cases of violation identified through the submission reports are as follows:

- Neglected to verify the purpose of transactions, occupations of customers, etc.
- Neglected to verify customer identity with valid principal identification documents
- Neglected to send transaction-related documents by registered mail that must not be forwarded or the like in non-face-to-face transactions

and so on.

The Ministry of Internal Affairs and Communications assesses that business operators that conduct non-face-to-face verification at the time of transaction, and other business operators with few workers that have not established a management system, in particular are high risk of being misused for ML/TF.

(b) Trends of STRs

There were 13 STRs from telephone forwarding service providers between 2017 and 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 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, 30.8%). There was STR about transactions suspected of being a spoofing contract where a person told business operators that they received a notice by mail about an unfamiliar contract. Also, there was a STR from a company after checking a customer's transactions in-house, triggered by inquiries from public institutions.

(c) Typologies

The following case is an example of misusing a telephone forwarding service for money laundering:

- In as 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 a means to conceal the owner of the criminal proceeds.

In addition, there were cleared cases which telephone forwarding service provider was arrested for aiding fraud where they provided telephone forwarding services for specialized fraud group while being aware that their services would be misused for specialized fraud.

B. 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. The Act also requires business operators to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

Furthermore, in addition to the supervisory measures based on that Act, 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

Furthermore, to ensure full compliance by telephone forwarding service providers, the Ministry of Internal Affairs and Communications holds briefing sessions for them and outlines the Act on Prevention of Transfer of Criminal Proceeds and important points of their obligations under the Act. In addition, the Ministry sends brochures to inform telephone forwarding service providers of verification at the time of transactions. It also explains 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, the Ministry sent an overview document of the Act on Prevention of Transfer of Criminal Proceeds to telecommunications carriers that providing telephone receiving services and telephone forwarding services to disseminate information that needed to be grasped. The document also described the items to be confirmed at the time of transaction.

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 November 2019, the Ministry issued a rectification order to one telephone forwarding service provider that was recognized as violating obligations of verification at the time of transaction, requiring the provider to fully understand and comply with laws related to verification at the time of transaction and creation of verification records, and to implement measures, etc. to prevent recurrence.

In addition, the Ministry undertakes written surveys to grasp the actual state of compliance with laws and regulations and of risk management by business operators. It also provides guidance and supervision, etc., relating to risks faced by respective business operators based on information obtained through such surveys, as well as from verification results relating to violations, etc.

The following matters are those identified by the competent authorities that business operators should note:

- Sending transaction-related documents by registered mail that must not be forwarded or the like in non-face-to-face transactions
- Checking corporate customers for beneficial owners
- Checking the purpose of transactions, occupations of customers, 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

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

Regarding specialized fraud crimes, there have been many actual cases of schemes such as misusing telephone transfer systems to deceptively show land-line numbers to counterparties, and sending postcards, etc. stating a request to make a call to a number simulating that of a public office. 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.

C. Assessment of Risks

By using telephone forwarding services, customers can give their business a false appearance and can conceal the principal of ML/TF or ownership of criminal proceeds. Considering this, it is recognized that telephone forwarding services present the risk of being misused for ML/TF.

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 business operators of their statutory obligations and mitigating the risk through guidance and supervision, including the abovementioned risk-mitigating measures and administrative responses.

However, the level of these efforts differs from one operator to the next, and business operators that are not taking effective mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and could affect the risk for the business category as a whole.

In addition, based on STRs, actual cases, etc., it is recognized that the transactions covered in *Section 5 High-risk Transactions*, transactions under anonymous or fictitious, borrowed names, and pseudonyms (including suspected ones) are likely to present 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 (hereinafter referred to as "legal/accounting 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 2020, 42,164 lawyers,7 Okinawa special members, 434 foreign lawyers, 1,302 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. As of the end of March 2020, 22,724 judicial scriveners and 741 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 scriveners registry kept by the Japan Federation of Certified Administrative Procedures Legal Specialists Associations. As of April 2020, 48,639 administrative scriveners and 727 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 registered foreign certified public accountants roster kept at the Japanese Institute of Certified Public Accountants. As of the end of March 2020, 31,793 certified public accountants, 2 foreign certified public accountants, and 245 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. As of the end of March 2020, 78,795 certified public tax accountants and 4,197 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.

---

*1 Legal/accounting professionals mean those listed in Article 2, paragraph 2, item 43 (lawyer or legal professional corporation), item 44 (judicial scrivener or judicial scrivener corporation), item 45 (administrative scriveners or administrative scriveners corporation), item 46 (certified public accountant or audit firm), and item 47 (certified public tax accountant or certified public tax accountants' corporation) of the Act on Prevention of Transfer of Criminal Proceeds.

Furthermore, the FATF and others have suggested that, as banks, etc. are implementing the regulations on ML/TF effectively, people who have been attempting to launder money or finance terrorism through banks in the past are changing their strategy. They are now starting to conduct ML/TF by obtaining professional advice from experts in legal/accounting fields, or by involving experts in legal/accounting fields who have high social credibility in their transaction activities.

(b) Typologies

The following cases are examples of misusing legal and accounting services for money laundering in Japan:

- A case where a loan shark asked an administrative scrivener to provide incorporation services 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
- A case where an innocent certified public tax accountant and a certified public tax accountants' corporation were used for accounting treatment of proceeds derived from fraud and gambling in order to disguise them as legitimate business profits
- A case where the offender asked a judicial scrivener, who was unaware of the situation, to set up a corporation using criminal proceeds obtained from fraud, etc. and also became the founder of such, after that opened a bank account in the company's name, and where criminal proceed was transferred into the account of legal person,

etc. 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 requires legal/accounting professionals, excluding lawyers, to conduct verification of customer identification data and prepare and preserve verification records and transaction records with regard to specified transactions.

In addition, the Act provides for supervisory measures by the competent authorities, such as requiring the submission of reports and reference materials from and conducting on-site inspection of legal and accounting professionals (excluding lawyers).

As for lawyers, the JFBA sets rules and regulations that stipulate the duties of lawyers. These include verification of client identity with regard to certain transactions, retention of records, and avoiding acceptance of instructions 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 profession are also making efforts to promote AML/CFT measures, such as by developing regulations, preparing materials about duties, providing training, etc., and through such endeavors promote understanding of ML/TF risks among professionals.

a 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. Furthermore, JFBA has created various tools and a Q & A to promote lawyers' compliance with JFBA's rules regarding AML/CFT measures, provides them to lawyers and bar associations. At the same time, examples of efforts at law firms and risks of money laundering caused by new technologies will be published in the magazine *Freedom and Justice* to make them known, thus supporting the reinforcement of AML/CFT measures by each lawyer.

The matters that JFBA should keep in mind when dealing with money laundering include the following:

- 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:

- Cases where a lawyer did not accept a Japanese enterprise's request, due to a high risk of money laundering when the enterprise without introduction inquired about payment via the law firm when sending money to a foreign company, since the business content of the Japanese company was not familiar to the law firm.
- Cases where risks are identified, evaluated, and mitigated, in the acceptance decision after inquiring the counterpart of the client's business or proposed project whether there is property to be transferred and whether the proposed transaction is standard with consideration of the client's business type. At the first interview, the lawyer confirms any financial difficulties or unusual points. In addition to independent and reliable public information sources, such as corporate registration, the lawyer uses public Internet information sources and inquiries.
- Cases of using domestic and foreign databases and investigating whether clients are antisocial forces or foreign PEPs in the decision to accept requests from clients.
- Cases of building an internal control system by creating and disseminating internal regulations and manuals related to ML/TF measures, training and briefing sessions for lawyers and staff, and establishing responsible departments, such as internal control committees in the law office.
- Cases of promoting clients' cooperation and confirming appropriately customer identity, where delegation contract and advisory contract templates stipulate that the law firm can request principle identification documents. The clients should notify if there is a change in customer identity.

b Japan Federation of Judicial Scriveners Association

The Japan Federation of Judicial Scriveners Associations 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, the Federation again ensured that its members complied with the Guidelines for Conducting Duties to Prevent the Transfer of Criminal Proceeds.

The Federation also based on the Articles of Association of the Judicial Scriveners since 2019 has 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) in accordance with the Article. Accordingly, the Federation monitors the verification of customer identification, creation of transaction records, etc., and status of storing such records, etc. (from July through December only in 2019 and January through December annually in and after 2020), while each Judicial Scriveners Association interviews members who are recognized as having risk based on the results of monitoring and reports from the members and require them to make corrections as necessary.

The matters that judicial scriveners should keep in mind when dealing with money laundering include the following:

- 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

In April 2018, the Japan Federation of Certified Administrative Procedures Legal Specialists Associations conducted a written survey of administrative scriveners on their status of compliance with the Act on Prevention of Transfer of Criminal Proceeds.

Furthermore, from March 2019, the Federation posted a document calling for an understanding of obligations, such as identity verification and the importance of preventing ML, on the website for administrative scriveners, based on the results of a fact-finding survey on work of administrative scriveners under the Act on Prevention of Transfer of Criminal Proceeds.

The matters that administrative scriveners should keep in mind when dealing with money laundering include the following:

- 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

The Japanese Institute of Certified Public Accountants 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 the Japanese Institute of Certified Public Accountants introduces e-learning training and publications related to ML published by FATF. Also, the April 2020 issue of the institutional magazine Accounting and Audit Journal carries an article entitled "Basics and Risk-Based Approach to Countermeasures against Money Laundering and Terrorism by Accountants."

The matters that certified public accountants should keep in mind when dealing with money laundering include the following:

- 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 administrative scriveners.

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

- Cases of concluding new contracts, where the risks are classified according to the contract destinations' business types, and the higher the risk, the more materials are used to examine the contracts.
- Cases of continuing audit contracts (renewed initially every year), where the types of industries, officers, significant shareholders, etc. are confirmed.
- Cases of conducting new contracts for specific industries where there are in-depth investigations based on past data.

e National Tax Agency and Japan Federation of Certified Public Tax Accountants' Associations

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, the Federation 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.

The following matters are those identified by the competent authorities that certified public tax accountants and certified public tax accountants' corporations should note regarding 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. The competent authorities evaluate that there is a risk that tax accountants will be used for ML/TF in cases including the following:

- Acts or procedures concerning buying and selling residential lots and buildings
- Acts or procedures concerning the establishment or merger of companies, etc.
- Management or disposal of cash, deposits, securities and other assets

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 a practical 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. Assessments may differ widely depending on the utility value and usage of the land. This difficulty in estimating the appropriate value of the property can be misused for ML/TF by artificially inflating a property's value beyond a reasonable price, and then paying the inflated 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 operators are taking, in addition to statutory measures as a matter of course, the abovementioned mitigating measures against these risks.

However, the level of these efforts differs from one operator to another, and business operators that are not taking effective mitigating measures corresponding to their risks may face an increased risk of misuse for ML/TF, and could affect the risk for the business category as a whole.

In addition, based on STRs, actual cases, etc., it is recognized that the transactions covered in *Section 5 High-risk Transactions*, transactions under anonymous or fictitious names, borrowed names, and pseudonyms (including suspected ones) are likely to present a higher risk.

2. Products and Services Utilizing New Technology that Require Further Examination of Actual State of Use, etc. (Electronic Money)[*1])

(1) Present Situation

The average monthly use of electronic money per household (household of two people or more) in Japan increased from 17,644 yen in 2017 to 20,567 yen in 2019. Meanwhile, the proportion of households (household of two people or more) using electronic money worth 10,000 yen or more increased from 24.6% in 2017 to 31.2% in 2019. In Japan, the use of electronic money has spread in the past few years (see Tables 15 and 16).

Regarding electronic money in Japan, most of it falls under prepaid payment instruments issued under the Payment Services Act. Prepaid payment instruments are certificates, etc., or numbers, markings, or other signs (including instruments for recording value in computer servers etc.) that are issued in advance for 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.

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, monetary value is changed 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 customer identification documents. Customer verification is often completed through only declaration of the customer's name and birth date on issuance. These characteristics give prepaid payment instruments high anonymity, so 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.

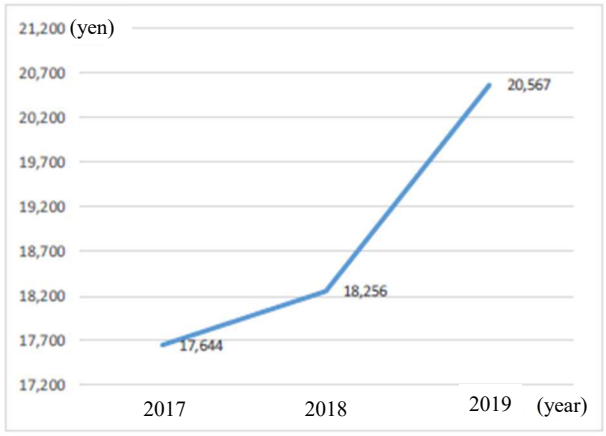
However, coupled with the progress of cashless society, there are many stores where electronic money can be used, including online stores. In addition to the fraudulent deception of electronic money (prepaid cards), there are cases where money laundering is conducted by transmitting a deceived electronic money number and selling the electronic money usage right to a purchaser.

---

*1 In this NRA-FUR, electronic money refers to a monetary value equivalent to cash transferred to a card, etc. It does not include credit cards, debit cards, post-paid cards or pre-paid cards such as bus cards used to purchase specific items and services.

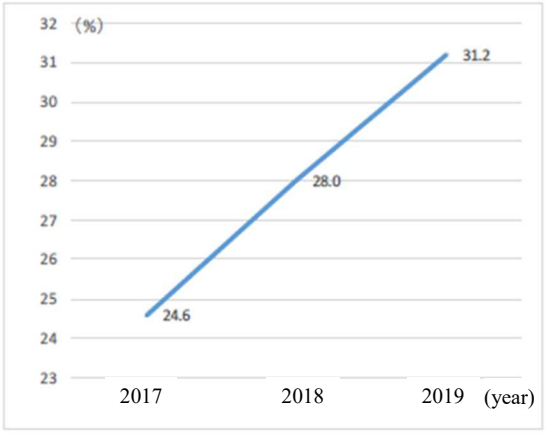
*2 Issuers of cards using the pre-paid payment methods whereby withdrawal or remittance is possible up to the charged value are equivalent to funds transfer service providers under the Payment Services Act, so they are designated as specified business operators under the Act on Prevention of Transfer of Criminal Proceeds. As such, they must conduct verification at the time of a transaction when issuing.

Table 15 [Change in Average Amount of Electronic Money Used per Household/Month (Households of Two or More People (2017–2019)]



Note: Data from the Ministry of Internal Affairs and Communications

Table 16 [Change in Rate of Households using ≥ 10,000 Yen in Electronic Money/Month (Households of Two or More People) (2017–2019)]



Note: Data from the Ministry of Internal Affairs and Communications

(2) Typologies

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

- A case where 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.
- A case where the usage rights for electronic money obtained through fraud were used to purchase usage rights for another brand of electronic money, the rights were resold to a purchase trader who then remitted the payment to an account under another person's name, after that the money in such an account was withdrawn from an ATM,
- A case where a specialized fraud group colluded with a liquor dealer. The specialized fraud group used electronic money that the specialized fraud group stole and purchased many beer tickets that the liquor dealer fictitiously put up on a shopping site. Then the specialized fraud group had the site operating company transfer the sales price to the account of the liquor dealer.
- A case where a purchaser received a deceived electronic money number by e-mail from a specialized fraud group and got the money.

and so on.

Of the 3,533 recognized cases of fraudulent billing fraud during 2019, 1,481 cases were conducted by the method of misusing electronic money, accounting for 41.9% of the total, and the amount of financial damage per case was approximately 800,000 yen. In illegal remittances related to Internet banking during 2019, it was recognized that there are methods such as illegal remittances to deposit and savings accounts as conventional, and purchasing electronic money, charging prepaid virtual credit cards, and purchasing electronic gift certificates from major e-commerce websites as new.

(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 used in the process of money laundering, and the number of cases is on the rise.

In Japan, however, as refunds of prepaid payment instruments are prohibited under the Payment Services Act, in principle, users cannot freely withdraw funds with respect to the charged value. In addition, under the present conditions, many issuers set an upper charge limit, and service locations are limited to specific member shops, 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 (prepaid cards) 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 (usage rights); (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, agencies and business groups 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 strengthened their initiatives to clarify the actual status of and dissolve such traders, etc. The police have cleared electronic money purchasers in violation of the Act on Punishment of Organized Crimes. Furthermore, as a countermeasure against the types of fraud in which electronic money is deceived, the police promote the prevention of damage in cooperation with related business operators, including convenience stores and electronic money issuing companies.

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

[Casinos]

While 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.
- ○ Casinos offer various financial services (accounts, remittance, foreign exchange, etc.).
- ○ In some jurisdictions, casinos are regarded as entertainment venues, rather than financial institutions, and are poorly regulated for AML/CFT.
- ○ 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,

and so on.

The Act on Development of Specified Integrated Resort Districts (Act No. 80 of 2018, hereafter referred to as the "IR Development Act") was enacted, and it is necessary to take appropriate AML/CFT measures in the casino business in the future. Having regard to the risk of casinos being misused for money laundering, FATF Recommendations request casino business operators to undertake customer due diligence measures including identifying and verifying the identity of customers when they establish business relations with a customer or carry out financial transactions equal to or above USD/EUR 3,000. Among other measures, it also states that casinos should be licensed to implement AML/CFT measures effectively.

Based on these recommendations, IR Development Act stipulates that the casino business must be conducted under license and added casino business operators to the list of specified business operators by revising the Act on Prevention of Transfer of Criminal Proceeds, which requires casino business operators to verify the identity of customers at the time of transaction, to prepare and store transaction records, to report suspicious transactions, and so on. Furthermore, the Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds, which was revised by the Order for Enforcement of the Act on Development of Specified Integrated Resort Districts promulgated in March 2019 (Act No. 72 of 2019, hereafter referred to as the "IR Development Order") added the following transactions to "specified transactions"

for which duties such as verification at the time of transactions are imposed:

- ○ 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 above-mentioned regulations, as AML/CFT measures under the IR Development Act and the IR Development Order, casino business operators must:

- ○ prepare the Regulations on Prevention of Transfer of Criminal Proceeds (examined by the Casino Regulatory Commission)

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

- submit a report to the Casino Regulatory Commission on the above-mentioned “specified transactions” where cash worth over 1 million yen is received or refunded
- 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,

and so on, to create an environment in which casinos will not be misused for money laundering.

Based on the IR Development Act, in January 2020 the Casino Regulatory Commission was established as an administrative committee of an external bureau of the Cabinet Office to implement strict regulation and supervision of casino business, including AML/CFT measures.

Section 5. High-risk Transactions

1. Transaction Types

By referring to cleared cases in which foreigners visiting Japan committed money laundering offences as well as situations that increase the risks of ML/TF (non-face-to-face transactions and businesses that are cash-intensive) as described in the FATF's 40 New Recommendations and its Interpretive Notes, we identified: (1) non-face-to-face transactions; (2) cash-intensive businesses; and (3) international transactions as the types of 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

With factors such as the development of information technology and improvement of services by business operators for customer convenience, non-face-to-face transactions through the internet and other facilities have been expanding.

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 mail-order 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 whether the customers have given false identification data or whether 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.

Incidentally, in the third round of FATF Mutual Evaluations, it was pointed out that customer identification and verification requirements for non-face-to-face transactions in Japan are insufficient.

(b) Typologies

The following cases are examples of misusing non-face-to-face transactions for money laundering:

- A case where a stolen health insurance card was misused to open a bank account in the name of another party through non-face-to-face transactions, and the account was misused to conceal criminal proceeds derived from selling stolen goods
- A case of fraud and underground banking, etc. where a person pretended to be a fictitious person and opened a bank account through non-face-to-face transactions, and the account was used to conceal criminal proceeds
- A case of internet banking-related illegal remittance, where several accounts opened in the name of a fictitious person through a non-face-to-face transaction using a falsified ID were designated as the remittance destinations
- A case where a bank account was opened through a smartphone by using identification documents with photographs of a long-estranged relative, and criminal proceeds from fraud was remitted to the account
- A case where a request to open a bank account was made online by using a fake health insurance card, and the cash card sent by registered mail that must not be forwarded was received by presenting the fake identification document used to open the bank account to the post-office clerk

- A case where an account was opened under a fictitious legal person's name online, and criminal proceeds from specialized fraud were remitted to the account,
- A case of utilizing a forged image of another person's driver's license to open a bank account in the person's name and applied for a loan contract with a money lender on the Internet, where the loan was transferred to the same account,

and so on.

B. Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds 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 methods of utilizing transfer-prohibited mail and person-limited receipt mail.

In recent years, however, 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 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 revised Act stipulating measures to mitigate risks was promulgated in November 2018 and took effect in April 2020.

The following is an overview of the revision:

- Regarding the identification documents to be sent to specified business operators in a customer identification measure where transaction documents are sent by mail that requires no forwarding, the businesses must receive one original document, or copies of two types of identification documents, or a copy of an identification document and a supplementary document indicating the current address (two pieces in total), instead of one copy of an identification document as previously required.
- As for a customer identification method where transaction documents are sent by registered mail with delivery restricted to the addressee, the types of identification documents that may be presented by customers at the time of transaction are limited to identification documents with photographs, instead of any type of identification document as previously required.

Also, along with this revision, another revision of the Act that introduces a mechanism for completing customer identification online was made as a customer identification method to support FinTech, and implemented on the day 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 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 images of the appearance of a third party taken 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 keeping customer identification sufficiently up to date.

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.

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 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 maintain high anonymity, 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 2014 the average monthly consumption expenditure of a household (2 or more people) using cash as the purchasing medium was 241,604 yen (82.5% of all consumption expenditure). For credit card, monthly installment payment, and credit purchases (hereinafter referred to as "credit card, etc."), the average amount was 46,995 yen (16.0% of all consumption expenditure). Although the ratio of expenditure in cash has been declining (93.5% in 2004, 88.8% in 2009 and 82.5% in 2014), purchases in cash still comprise the largest proportion of expenditure by means of purchase (see Table 17). Use of cash in Japan is higher than that in other countries (see Table 18).

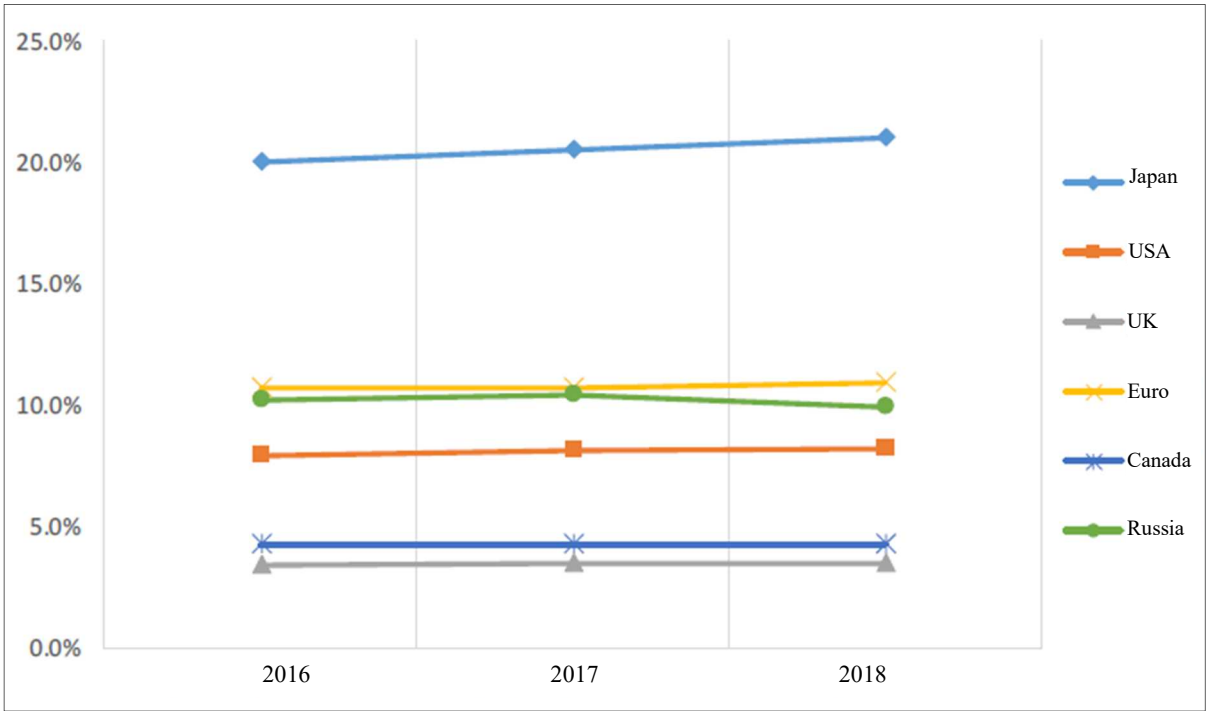
As for the characteristics of cash transactions, unlike currency exchange transactions, which are a quick way to transfer funds to remote places, a certain amount of time is required to transfer cash because of necessity of physical movement. On the other hand, cash has high liquidity and transfer of ownership is easy. Along with that, cash transactions are highly anonymous unless they are recorded, resulting in low visibility in terms of tracing the flow of funds.

Table 17 [Expenditure by Type of Purchase (Households of Two or More People/Monthly Average)]

Consumption expenditure	2004			2009				2014			
	Cash	Credit card, etc.	Total	Cash	Credit card, etc.	Electronic money	Total	Cash	Credit card, etc.	Electronic money	Total
Expenditure amount (yen)	299,340	20,724	320,063	267,119	32,574	1,244	300,936	241,604	46,995	4,283	292,882
Ratio (%)	93.5%	6.5%	100.0%	88.8%	10.8%	0.4%	100.0%	82.5%	16.0%	1.5%	100.0%

Note: Data from the Ministry of Internal Affairs and Communications

Table 18 [Ratio of Cash Distribution Balance for Different Countries in Nominal GDP (2016–2018)]



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. In addition, it is recognized that crime organizations conceal criminal proceeds in cash. There have been some actual cases where large amounts of cash which are criminal proceeds from gambling offenses, loan-shark crimes, etc. concealed in safes managed by crime organization, were confiscated.

There was another case of an international money laundering offense where an international criminal organization withdrew a large amount of cash in one lump sum and remitted the proceeds from fraud committed overseas to a financial institution in Japan, 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 the criminal proceeds obtained through smuggling gold bullion without permission from the Director-General of Customs was caught. Another cleared case involved an offender attempting to take cash obtained from specialized fraud out of Japan as checked luggage for air travel without declaring it to the Directors-General of Customs.

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

- A case where offenders obtained cash by selling or pawning stolen items in the name of a fictitious or another party at secondhand shops, pawnshops, etc.
- A case where 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,

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

- A case where 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
- A case where an offender deposited some of the cash obtained through armed robbery into an account multiple times in a short period under the name of his/her acquaintance via an ATM
- A case where an offender transferred cash derived from the sale of a car obtained through fraud to a foreign country using a fund transfer service provider
- A case where 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,

and so on.

B. Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds requires specified business operators who operate financial businesses, etc. to conduct CDD. This includes verification at the time of a transaction and preparation and preservation of verification records and transaction records when they conduct transactions that accompany receipt and payment of cash of more than 2 million yen (100,000 yen in the case of transactions that accompany exchange transactions or the writing of a cashier's check). The Act also requires specified business operators to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

In addition, the Secondhand Articles Dealer Act and the Pawnbroker Business Act stipulate that the address, name, etc. of the counterparty shall be verified at the time of transaction. As for cash couriers, when exporting/importing cash, etc. equivalent to over 1 million yen (or 100,000 yen for export to North Korea) in

person, the 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, which are considered to be measures that contribute to reducing the risks associated with cash transactions.

The Japanese government is pushing for improved convenience and efficiency through the spread of cashless payments under the Japan Revitalization Strategy 2016 (Cabinet decision on June 2, 2016), etc. and has presented its plan to promote cashless payments in the lead up to the 2020 Tokyo Olympic and Paralympic Games, etc., aiming to increase the ratio of cashless payment to around 40% by 2025. It is expected that promoting cashless payments will lead to the revealing of hidden cash assets, suppression of hidden cash distribution, etc., and reduction of money laundering involving cash transactions, etc.

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 business operators should pay special attention. The list illustrates cases focusing on forms of cash usage, such as:

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

and so on.

Business operators are putting measures in place to ensure STRs in light of the above.

- For cash deposits and withdrawals that exceed a certain level, a hearing sheet is issued at the teller, and STRs are submitted if necessary.
- 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.
- Business operators are also implementing other measures to mitigate risk, such as refusing to conduct overseas remittances using cash brought in to the premises by a customer whose identity has not been verified because he/she does not hold an account, etc.

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 2019, Japan's economy was the third largest in the world in terms of nominal GDP (approximately 553.7 trillion yen), the fourth largest in terms of overall import value (approximately 78.5995 trillion yen, and the fifth largest in terms of overall export value (approximately 76.9317 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 accept systems that allow directors and shareholders legal person without transparency to be registered under the names of third parties. This situation is recognized as where 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 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's financial institution etc., there is a risk that money laundering could occur unless the correspondent's institution 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 offences by international criminal organizations in which proceeds from fraud committed abroad are transferred to financial institutions in Japan. Multiple factors are thought to have caused this, including trust in Japan by the international community, the high reliability of Japan's financial systems, and the time difference between countries where damage occurred, which is used to delay the detection of crimes.

Besides the abovementioned exchange transactions, etc. based on correspondent banking relationships, cash couriers may be misused for ML/TF in international transactions.

Also, international attention on 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, duly considering overseas trends such as supervisory oversight by foreign authorities as well as domestic ones.

(b) Typologies

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

Analysis of the trends of cleared cases of money laundering involving visiting foreigners reveals that Chinese and Vietnamese rank highly in terms of the number of foreigners who are perpetrators of cleared cases by nationality. Recognized predicate offenses include theft, fraud, Violation of the Immigration Control and Refugee Recognition Act, and computer fraud. 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.

There have also been other cases in Japan of misusing transactions for money laundering, such as:

- A case where proceeds derived from instances of fraud committed in the United States and Europe were remitted to accounts opened at Japanese banks, and Japanese nationals who were the account

holders withdrew the funds by disguising the transactions as legitimate ones by presenting forged bills and other documents at the banks' counters

- A case where 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.

As recognized in these cases, international crime organizations have recently been conducting international money laundering using a modus operandi in which they use accounts at financial institutions in Japan as ones for remitting money stolen in fraud cases conducted in other countries, and an accomplice in Japan withdrew the stolen money by disguising it as money remitted in a legitimate transaction.

The following are the main characteristics of these money laundering cases where the true source of funds, their owner, 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
- There may be a request to pay out almost all the remitted amount in cash
- The remitters often request reverse transactions later.

In addition to the above, there was a case where the offender opened an account in advance at a branch of a local financial institution whose head office is in a distant, giving a fictitious reason for opening the account in order to conceal criminal proceeds from overseas.

Moreover, the following international money laundering case was recognized.

- 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.

There were also cases of foreigners in Japan who operated underground banking, such as a case where illegal overstayers, etc. use money laundering to remit criminal proceeds, etc. overseas. Although the number of cleared cases has been trending downward since 2014, there was a cleared organized crime case where illegal remittance of money exceeds 2 billion yen. It is impossible to deny that criminal proceeds from fraud, drug offenses, etc. are illegally remitted to other countries by via underground banking. For this reason, the modus operandi of unlicensed international remittance businesses requires focused attention. In recent years, the modus operandi has been sophisticated, with offenders converting the form of criminal proceeds from cash to goods, and then back to cash again to disguise transactions as legitimate transactions. The following are examples of such cases using sophisticated modus operandi:

- A case where money requested by a customer for remittance was used to purchase used cars for which there is strong demand in the offender's home country, and the cars were exported by disguising them as goods in legitimate transactions that were 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 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 was remitted by a customer into an account opened in a foreigner's name and subsequently paid out in cash. The cash was handed over to a domestic company run by the foreigner, and the company purchased Japanese products using the cash as funds, subsequently exported the products, and obtained foreign currency from selling them abroad. This arrangement was in effect equivalent to an international remittance
- A case where money was remitted by a customer into an account opened in another person's name, and cash withdrawn from the account was smuggled out to another country in a travel bag
- A case where a criminal group formed by a study-abroad broker and foreigners in Japan operated large-scale underground banking in which accounts managed in and outside Japan by the group, etc.

were opened under the assumption of being used for remittances and payment to families, etc. of foreign students, etc. living in their home countries, without actually transferring funds,

and so on. In addition, the following are examples in other countries.

- A case where criminal proceeds were internationally transferred through cross-border smuggling of a large amount of cash and through transactions in which premiums over the actual product prices were paid,

and so on.

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. 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[*1]; 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.

The Financial Services Agency's Guidelines for Supervision provides that one of the focal points for supervision is whether business operators have developed internal control systems related to correspondent banking relationships, such as:

- 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 explains in detail specific inspection

---

*1 For example, the following obligations are imposed:
- the obligation to verify that the other parties to correspondent banking relationships have an internal control system necessary to conduct verification at the time of transactions appropriately;
- the obligation to verify that the other parties to correspondent banking relationships have not formed relationships to continuously or repeatedly perform exchange transactions with any financial institution, etc. that does not have an internal control system necessary to conduct appropriate verification at the time of transactions; and
- the obligation to collect information on the AML/CFT systems developed by other parties to correspondent banking relationships, their business activities, and the status of supervision provided by administrative authorities in their respective countries, and the obligation to clarify the responsibility of each party in conducting verification at the time of a transaction,

as mentioned above.

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

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.

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.

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

- Interviewing corporate customers who start foreign exchange trading, including checks on business details by visiting the corporation.
- Rejecting overseas remittance transactions of customers bringing in cash.
- Strengthening verification at the time of transaction for overseas remittance for areas close to countries and regions for which countermeasures were requested from member countries in the FATF statement.
- Submitting by focusing on the discrepancy between the purpose of remittances from foreign countries and the recipients' actual usage of funds.

C. Assessment of Risks

Compared with domestic transactions, international transactions can make it difficult to track ML/TF because domestic legislation and transaction systems, etc. vary from country to country.

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 from such cases will be returned overseas and apply countermeasures.

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.

2. Countries/Regions and Risks

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 assessment or detailed NRA-FURs 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 that jurisdiction. 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 its 40 New Recommendations (Recommendation 19), in October 2019 the FATF asked its members to strengthen their financial oversight of branches and subsidiaries of financial institutions based in Iran to introduce a stricter 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. Iran has not enacted a collateral law to conclude the United Nations Convention against Transnational Organized Crime or the International Convention for the Suppression of the Financing of Terrorism, both of which conform with FATF standards. Accordingly, since February 2020, the FATF has been requesting all FATF members, other countries, and regions to lift the suspension of countermeasures against Iran completely.

In addition, FATF public statements used to identify jurisdictions[*1] other than Iran and North Korea, and ask members to take AML/CFT measures in consideration of risks arising from deficiencies associated with those jurisdictions; however, no such jurisdictions were mentioned in the statement of June 30th, 2020.

(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 the 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 that specified business operators must, upon conducting a specified transaction with a person who resides or is located in a specified jurisdiction and any other specified transactions that involve transfer

---

*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.

of property to a person who resides or is located in a specified jurisdiction, conduct strict checks of the source of wealth and source of funds as well as customer identification data, etc.

(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 were mentioned in the statement released on June 30th, 2020. Even so, the FATF published the names of countries/regions that have serious strategic deficiencies related to AML/CFT measures and have developed action plans to deal with them as countries/regions that continue to improve the compliance with 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. 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 a transaction.

[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 (2018 to 2020) 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 June 2020 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	2018			2019			2020	
	Feb	Jun	Oct	Feb	Jun	Oct	Feb	Jun
Iran	◎	◎	◎	◎	◎	▲	●	●
North Korea	●	●	●	●	●	●	●	●

[Countries/regions designated in the FATF's monitoring process for improved observance of AML/CFT measures]

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

Countries/regions and period	2018			2019			2020	
	Feb	Jun	Oct	Feb	Jun	Oct	Feb	Jun
Albania							○	○
The Bahamas			○	○	○	○	○	○
Barbados							○	○
Botswana			○	○	○	○	○	○
Cambodia				○	○	○	○	○
Ghana		○	○	○	○	○	○	○
Jamaica							○	○
Mauritius							○	○
Myanmar							○	○
Nicaragua							○	○
Pakistan		○	○	○	○	○	○	○
Panama					○	○	○	○
Syria	○	○	○	○	○	○	○	○
Uganda							○	○
Yemen	○	○	○	○	○	○	○	○
Zimbabwe						○	○	○
Ethiopia	○	○	○	○	○			
Iceland						○	○	○※
Iraq	○							
Mongolia						○	○	○※
Serbia	○	○	○	○				
Sri Lanka	○	○	○	○	○			
Trinidad and Tobago	○	○	○	○	○	○		
Tunisia	○	○	○	○	○			
Vanuatu	○							

* For Iceland and Mongolia, the action plan was completed by the FATF statement dated June 30, 2020.

However, both countries substantially completed its action plan, on-site-visit remains in place to sustain due to the Covid-19 situation. For the situation in each country, refer to the original text of the statement,

Jurisdictions under Increased Monitoring – 30 June 2020

(https://www.mof.go.jp/international_policy/convention/fatf/fatfhoudou_20200722_3.pdf).

3. Customer Attributes and Risks

We identified, analyzed, and assessed the customer types that affect transaction risks by referring to cleared cases in which members of organized crime groups committed money laundering and severe terrorism situations; circumstances that increase the risks of ML/TF listed in the FATF's Interpretive Note to the 40 New Recommendations ("non-resident customers" and "ownership structures of companies that appear unusual or excessively complex"); the matters pointed out in the Third Round Mutual Evaluation of Japan by the FATF ("financial institutions are not required to take specific steps to mitigate the increased risk accompanying dealings with PEPs," and "customer identification documents upon which financial institutions are permitted to rely does not include photographic identification [or additional secondary measures to mitigate the increased risk accompanying such situations]") 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 without transparency of beneficial owner

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

A. Factors that Increase Risks

(a) Characteristics

In Japan, Boryokudan and other anti-social forces[*1] 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, 2020, 24 groups are listed as designated Boryokudan under the Act on Prevention of Unjust Acts by Organized Crime Group Members.

As at the end of 2019, the total number of Boryokudan gangsters was 28,200,[*2] including 14,400 Boryokudan members and 13,800 associates. The totals of these numbers have been declining continuously since 2005. 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.

In addition to extortion and compulsion targeting companies and administrative organs, armed robbery, theft, etc., Boryokudan also commit various crimes to obtain funds according to changes in the times, such as specialized fraud and other types of fraud that misuse various public benefit systems. These days, new crimes to obtain funds, such as cases of gold bullion smuggling, are emerging. However, traditional crimes to obtain funds, such as extorting money from restaurants, etc. in downtown in the name of protection fees still remain as important sources of revenue for Boryokudan. Moreover, Boryokudan commit 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 who are substantially involved in their management or colluding with persons who cooperate with or assist in the money-making activities[*3], etc. of Boryokudan to conceal their actual state, and their funding activities have become more crafted. It is increasingly difficult to define them. Furthermore, they often launder money and disguise the relationship between fundraising activities and their results in order to avoid taxation on or confiscation of gained funds or to avoid arrest for obtaining the funds. Criminal proceeds are funds to maintain and strengthen

---

*1 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.

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

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

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 runaway tribes 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.

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.

(b) Trends of STRs

There were 1,258,000 STRs from 2017 to 2019, including 176,859 reports (14.1% of total reports) related to Boryokudan gangsters.

(c) Typologies

There were 1,409 cleared cases of money laundering from 2017 to 2019, including 173 cases (12.3% of total cases) related to Boryokudan gangsters.

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

- A case where Boryokudan concealed ownership of criminal proceeds obtained through fraud, including specialized fraud, illegal money-lending business, drug offences, offenses against the Worker Dispatching Act, etc., by using an account in the name of another party, etc.

Although the above type of case is often seen, the following are also observed.

- A case where Boryokudan received criminal proceeds in the name of protection fees, contributions, etc., by taking advantage of their organization's threatening behavior
- A case where a Boryokudan member knowingly received criminal proceeds generated from prostitution transferred to an account in the name of his/her relative
- A case where 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 an employee of the company providing the service to an account opened by the offender's acquaintance under the name of a dummy corporation
- A case where a Boryokudan member used an account opened by his wife under her maiden name as a repayment account for a loan shark

Case examples of quasi-Boryokudan's fund-raising activities include:

- Cases where quasi-Boryokudan-related members acted as lawyers and deceived cash from older people in the name of avoiding proceedings related to troubles.

- Cases where quasi-Boryokudan-related members acted as trading company employees and deceived cash from older people to solve problems related to name lending for use in purchasing bonds.
- Cases where quasi-Boryokudan-related members pretended to be real estate-related company employees, offered false acquisition stories to landowners, and deceived cash in the name of expenses related to land sales contracts.

B. 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, including companies other than specified business operators, to cut any relationships with anti-social forces.

Based on the situation mentioned above, the Financial Services Agency requires deposit-taking institutions, etc. to develop a system to cut relationships with anti-social forces in the Agency's Guidelines for Supervision, etc. The system includes institutional responses, development of an integrated management system, proper before-and-after screening and review, and efforts to dissolve business relationships.

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 business operators regularly screen their customers using domestic and overseas databases at the start of transactions even after the start of transactions. In the case of customers falling under antisocial forces, such as Boryokudan and quasi-Boryokudan, STRs are reported.

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.

C. 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. Thus, 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 terrorism issues remain severe, with terrorist attacks occurring in 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 has increased and become more complicated in terms of terrorist financing. Thus, in this NRA-FUR, we refer to the FATF Recommendations, its Interpretive Notes, the FATF's reports, and measures under the Act on Prevention of Transfer of Criminal Proceeds to take 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)

In taking up the above for discussion

- and comprehensively considering factors including the impacts of the above factors on Japan, we 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.

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. In September 2019, a statement by leader Abu Bakr al-Baghdadi was issued. He once again called on his supporters to step up all activities, including attacks and dissemination. 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 the U.S. and European countries etc. participating in the anti-ISIL coalition. For such attacks, ISIL called for fighters to use knives, vehicles, etc. to carry out terrorism when explosives or firearms were unavailable. In 2019, a terrorist attack by those believed to have been influenced by radical ideas, including ISIL's, occurred.

Besides, ISIL lost its territory in Iraq and Syria. As a result, foreign fighters and some of their families in both countries seemed to have left the area. It is considered that the perpetrators of the coordinated simultaneous terror attacks in Paris, France in November 2015 and the serial terror attacks in Brussels, Belgium in March 2016 have a history of travel to Syria, and there are concerns that foreign fighters will continue to conduct terrorist attacks in their home countries or third countries in the future.

Hamza bin Laden, a son of Osama bin Laden (the leader when AQ was organized), is using the Internet to call for Muslims around the world to carry out terrorism. He was allegedly killed in a US operation. However, the current leader, Ayman al-Zawahiri, has repeatedly insisted on anti-American and anti-Israeli ideas. Also, as AQ-related organizations operating in the Middle East, Africa, South West Asia regions, etc. have been committing terrorism targeted at local government organizations and the like and calling for fighters to practice terrorism in Europe and North America through online newsletters, etc., AQ and its related organizations are still a threat.

(b) Characteristics

On the other hand, the United Nations Security Council has adopted resolutions (No. 1267 and succeeding resolutions as well as No. 1373) to freeze the assets of or take measures against persons who are related to AQ or other terrorist groups. However, to date no person of Japanese nationality or residency has been included in this list 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.

In light of the matters related to the threat of and vulnerability to terrorist financing that have been identified internationally, we may cite the following as characteristics of terrorist financing:

- 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.
- Money intended for terrorist financing is sent to Iraq, Syria, and Somalia. However, in some cases, money is transferred through Turkey or other neighboring countries instead of going there directly.

The FATF also has asked its member countries to prevent nonprofit organizations[*1] from being misused by terrorists, etc. Of course, not all nonprofit organizations are inherently 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 funds raised for legitimate purposes are diverted into illegal channels.

Also, according to the Recommendations and Interpretative Notes etc., nonprofit organizations have the following vulnerabilities to terrorist financing:

- Nonprofit organizations enjoy the trust of the general public, have access rights to considerable sources of funds, and often handle large amounts of cash
- Nonprofit organizations conduct activities in the regions exposed to terrorist acts and their surroundings, and some of them provide systems for financial transactions
- In nonprofit organizations, the party responsible for raising funds and the party responsible for disbursing funds for their activities may be different, and the purpose for which money is spent may become 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.

---

*1 The FATF defines a nonprofit organization as a corporation, 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.

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 evidence to date of Japanese nonprofit organizations being misused for terrorist financing, we need to consider indications from nonprofit organizations overseas when engaging in financial transactions, etc. in light of the position, roles, etc. of Japan as an international financial market.

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[*1] 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 forms of material 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) Trends of STRs

STRs suspected of being related to terrorist financing have been filed by specified business operators. Some were reported after a transaction was found to have been made with the same name as an individual who is subject to asset freezing and other measures, or an individual who has been linked to terrorist groups. Others were reported after business operators looked at the customer type, transaction method, etc., and determined that the transaction might be related to terrorist funding. Most of the transactions filed were international transactions, many of which were transactions with countries/regions in Asia and the Middle East. Based on paying attention to customer attributes, there are STRs where debit cards are used to withdraw large amounts of cash multiple times in the above countries and regions.

(d) Domestic Case

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

- A rifle scope, which needed an export license issued by the Minister of Economic, Trade and Industry, was exported to Indonesia without the license. In this case, two Indonesians living in Japan were arrested for violating the Foreign Exchange Act (unlicensed export). Images that showed that the

---

*1 For countries and regions where terrorist organizations are active, refer to the list of persons subject to measures, such as asset freezes, following the United Nations Security Council resolutions (No. 1267 and its successors and No. 1373).

suspect seemed to resonate with Islamic extremist ideas and videos about the production of explosives were stored on the suspect's personal computer.

- In one cleared fraud case, a corporate executive was cleared for opening a bank account for the purpose of allowing a third party to use it and for stealing a cash card. Money was deposited in the account by an organization in Japan that was deemed to have been supporting Japanese Red Army[*1] members on the international wanted list, and almost all of the deposited money was withdrawn in a foreign country.

(e) Overseas cases

Furthermore, the cases in foreign countries introduced in the FATF report[*2] are listed below for reference. These cases contribute to the understanding of the actual situation of terrorist financing

- Self-financing/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 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 at the restaurants would later be used to print leaflets, books, make flags, and record 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 whose aim was to recruit and facilitate FTFs 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, a terrorist organization recruited an IT specialist to support terrorist activities through the internet. He was arrested for engaging as an IT expert, assisting his partners, breaking into online-based MLM (Multi-Level Marketing)/investment. As a result of the hacking activity, the terrorist organization managed to obtain some 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 account, several cash transactions were then carried out in favor of the terrorist organization members. In the end, the IT specialist was convicted for terrorist involvement by financially supporting a terrorist organization in Indonesia.

---

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

*2 Financing of Recruitment for Terrorist Purposes（January 2018） and Emerging Terrorist Financing Risks（October 2015）

- 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 5000 Israeli new shekels (equivalent to approximately 1,250 U.S. dollars).

- Misuse of Donations (Egypt)

  In 2013 a group of terrorists stopped two police buses and killed 24 police officers in Egypt. The Egyptian authorities arrested the involved terrorists. Afterward, the investigations revealed that a member of this cell operated a fake charity in a small town 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-assets, 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 tweets. 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, Amin tweeted a link to an article he had written entitled “Bitcoin wa’ Sadaqat al-Jihad” (Bitcoin and the Charity of Jihad). The article discussed how to use bitcoins and how jihadists could utilize this currency to fund their efforts. The article explained what bitcoins were, how the bitcoin system worked and suggested using a new tool, which keeps the user of bitcoins anonymous.

B. Measures to Mitigate Risks

(a) Statutory measures

Legislative measures to mitigate risks related to the abovementioned characteristics of 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 terrorist financing, which has been pointed out internationally, 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.

This Act defines murder, hijacking and other crimes committed for the purpose of threatening the general public, national or local governments, or foreign governments as the Criminal Acts to Threaten the General Public (Article 1) and sets forth punishments for providing funds or other benefits to carry out Criminal Acts to Threaten the General Public (Articles 2 to 5).

In addition to providing funds, providing land, buildings, property, services and other benefits to supporters who attempt to supply funds, etc., to terrorists who plan to commit Criminal Acts to Threaten the General Public are subject to punishment under the Act.

○ **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 August 9, 2020, 403 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 individuals and entities subject to them under the Act on Special Measures Concerning International Terrorist Assets-Freezing, which took effect in October 2015. Specifically, as of August 9, 2020, the names of 403 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, the Act on Special Measures Concerning International Terrorist Assets-Freezing, etc. Conducted by the Government Taking into Consideration United Nations Security Council Resolution 1267, etc. was amended to add virtual currency (crypto-assets) to the regulated assets with respect to gifts to international terrorists, etc., and the revision took effect in April 2017.

(b) Anti-terrorist efforts

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

While the key to 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

C. Assessment of Risks

Japan has been implementing the abovementioned anti-terrorist 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 in accordance with 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 identified 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 or 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 businesses can be abused in a way that avoids monitoring by business operators.

In particular, it is acknowledged that there is a high risk of terrorist financing when conducting transactions with people who are considered to be Islamic extremists.

Moreover, as terrorism has the characteristic of being a highly secretive activity and most of the terrorism-related information collected is fragmented, it remains 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 FATF Recommendations, the FATF states that non-resident customers potentially present a high risk.

Business operators may have transactions with non-resident customers, such as foreigners who do not have an address in Japan. However, there are usually limitations on confirming the main assets and income sources of non-residents and their identifications. Therefore, customer due diligence measures are restricted compared to those for residents. Furthermore, non-residents who trade through mail, the Internet, etc. while staying in a foreign country conduct non-face-to-face transactions in order to maintain a high level of anonymity. Tracking funds is even more difficult when ML/TF is conducted.

In the Interpretative Note of FATF Recommendations, the FATF states that non-resident customers potentially present a high risk.

B. Measures to Mitigate Risks

The Financial Services Agency's Guidelines for Supervision require business operators to develop internal control systems for suitable examination and judgment in order to file STRs. Such controls include detailed consideration of customer types and the circumstances behind transactions.

C. Assessment of Risks

In the case of transactions with non-resident customers, business operators have limited measures to conduct ongoing CDD compared with customers residing in Japan. Furthermore, when non-face-to-face transactions are conducted, 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 PEPs (the FATF lists heads of state, senior politicians, senior government, judicial or military officials, etc. as examples) have positions and influence that can be misused for ML/TF. Other than that, business operators' CDD, including verification of customer identification data and having a grasp of 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 to cope with corruption varies from jurisdiction to jurisdiction.

The FATF requires 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 have become international phenomena that can affect any society and economy. Countries have come to recognize that a comprehensive approach, including international cooperation, is necessary to promote efficient measures to prevent corruption. The international community is calling for measures to prevent the transfer of proceeds derived from corruption by foreign public officials. Thus, 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 in recent years. These cases include the following cases:

- 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 case where 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 case where 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 case where 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.

B. Measures to Mitigate Risks

When specified business operators conduct specified transactions with (1) the head of state 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), the Act on Prevention of Transfer of Criminal Proceeds, Enforcement Order and Ordinance require that the business operators conduct enhanced CDD, including verifying the source of wealth and source of funds as well as customer identification data, etc.

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. listed 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, we recognize that transactions with foreign PEPs may carry a high risk of ML/TF.

(5) Legal Persons without Transparency of Beneficial Owner

In the FATF's report[*1] released in 2018, the FATF pointed out that the recent advancement of globalization in economic and financial services offers criminals opportunities to misuse the structure of a company and business to conceal the flow of proceeds and criminality. For example, they conceal illegal proceeds as trading transactions by companies and misuse a dummy or obscure legal person, the nominee system, 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 over company assets according to their respective positions.

Hence, if property is transferred to a legal person, it enters a complex rights/control structure of a legal person, meaning it can be easy to conceal a natural person who has substantial ownership of the property.

Furthermore, by controlling a legal person, it is possible to transfer large amounts of property frequently in the name of corporate business.

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 [*2], 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 19).

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 20).

---

*1 Concealment of Beneficial Owner (July 2018)

*2 Under the Companies Act (Act No. 86, July 26, 2005) and the Act on Arrangement of Relevant Acts Incidental to Enforcement of the Companies Act (Act No. 87, 2005), one of the types of company provided prior to the Acts, limited liability company (*yugen-kaisha*), is no longer available. Limited liability companies (*yugen-kaisha*) existing as of the enforcement date of the Acts continue to exist as stock companies, and are referred to as "special limited liability companies" (*tokurei-yugen-kaisha*). There are special provisions in the Acts, such as that the name of a special limited liability company (*tokurei-yugen-kaisha)* shall include the term "*yugen-kaisha*."

Table 19 [Number of Corporations by Major Corporate Type in Japan (2016-2018)]

Category \ Year	2016	2017	2018
Stock company	2,520,823	2,537,667	2,554,582
General partnership companies	3,794	3,814	3,371
Limited partnership companies	17,042	16,112	14,170
Limited liability companies	66,045	82,931	98,652
Others	64,329	66,103	67,774
Total	2,672,033	2,706,627	2,738,549

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.

Table 20 [Number of Registered Establishments by Each Major Corporate Type (2017-2019)]

Category \ Year	2017	2018	2019
Stock company	91,379	86,993	87,871
General partnership companies	104	87	48
Limited partnership companies	58	52	47
Limited liability companies	27,270	29,076	30,566
Total	118,811	116,208	118,532

Note: The statistics of the Ministry of Justice.

Cleared cases of domestic money laundering offences 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, those that obscure the misuse of dummy legal persons or other legal persons make it difficult to track subsequent proceeds because the status of their activities or beneficial owner is unclear. Specifically, the following are example cases:

- A dummy legal person is established for the purpose of misusing it to conceal criminal proceeds
- A person who intends to conceal criminal proceeds illegally obtains a legal person owned by a third party.

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

Of the money laundering offenses arrested from 2017 to 2019, 36 offenses took advantage of unrealistic or opaque corporations. Similar offenses have been increasing in number in recent years. Of these, 14 offenses took advantage of unrealistic or opaque corporations in 2019. The number of corporations abused was 19. Looking at these corporations by type, there were 13 stock companies (including special limited liability companies), 3 limited liability companies, 2 limited partnership companies, and 1 different corporation type. Comparing with the number of corporations by major type in Japan (see Table 19), it can be seen that the ratio of limited partnership companies and limited liability companies is higher than that of stock companies.

Furthermore, among the above, corporations 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 for professionally and systematically committed crimes that generate large amounts of money.

Moreover, it is said that in so-called offshore financial centers, referring to countries/regions where financial services are provided to foreign corporations and nonresidents on a disproportionate scale relative to their economic size and at low tax rates, it is easy to develop various investment schemes 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. 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 services, it is possible to establish and maintain a legal person that has no physical presence. Specifically, this is done by providing others with an address or a telephone number that is not actually used by the legal person and making up fictitious or exaggerated appearances of business trustworthiness, business scale, etc., including corporate registration.

(b) Typologies

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

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

- A case where 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 proceeds from prostitution were concealed in the account as legitimate business proceeds

- A case where 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 case where 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

- A case where criminal proceeds from fraud, etc. committed in foreign countries were remitted to an account in the name of a dummy legal person

- A case where 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

- A case where 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

- A case where 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

and so on.

B. 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 under the Act on Prevention of Transfer of Criminal Proceeds, Ordinance for Enforcement of the Notary Act, Companies Act, etc. as systems to verify information on beneficial owners of legal persons.

The Act on Prevention of Transfer of Criminal Proceeds and its Ordinance specify the following as beneficial owners: (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; (2) 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 of a legal person to which the principle of capital majority rule does not apply; (3) a natural person who is deemed to have substantial impact on the business activities of a legal person; and (4) a natural person who represents a legal person and executes its business. The Act requires specified business operators to verify the identity of a customer's beneficial owner if the customer is a legal person.

Also 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 stock companies, general incorporated associations, and general incorporated foundations to report to notaries the identity of a natural person who is to be 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.

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[*1]. This is a system intended to mitigate the risk of dormant companies that have been resold or whose registration has been illegally changed from being misused for crimes. Dissolution of dormant companies has been occurring every year since FY2014, with approximately 18,000 cases in FY2017, 25,000 cases in FY2018, and 33,000 cases in FY2019.

In addition, the Act on Prevention of Transfer of Criminal Proceeds requires service providers who provide business addresses, other addresses of facilities and means of communication, and administrative addresses to the abovementioned legal persons, etc. to conduct CDD. This includes verification at the time of conducting transactions, and preparing and preserving verification and transaction records when they conclude service contracts. The Act also requires business operators to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like. They must do this by taking into account the contents of this NRA-FUR, in addition to the results of verification at the time of transactions and the modes of the transactions as well as other relevant circumstances, and comparing with the modes of ordinary transactions and the like.

C. Assessment of Risks

It is easy to conceal the identity of a natural person who has substantial ownership of property by placing that property in the complex rights/control structures of legal persons. Such characteristics of legal persons make it difficult to track funds owned by legal persons and obscure beneficial owner.

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.

---

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

Considering this, it is recognized that transactions with legal persons that do not have transparent beneficial owner present a high risk for ML/TF.

[Customers Who Use an Identification Document without a Photograph]

○ Risks specific to identification documents without a photograph

Regarding customer identification documents for verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds, Article 7 of the Ordinance stipulates that identification documents without a photo of the person to be verified (hereinafter referred to as "non-photographic ID") such as health insurance cards and registered seal certificates, may be accepted as identification documents within certain limits, as well as identification documents carrying a photo (hereinafter referred to as "photographic ID") such as driver's licenses, Individual Number Cards, and passports.

In the case of photographic ID, business operators can compare the photo on the ID and the appearance of the customer in front of them to confirm their identity.

On the other hand, the reliability of identification by non-photographic ID is lower than that by photographic ID. However, non-photographic ID is also issued only to the person to be verified, and it does help in identifying whether the person to be verified is the person who is carrying it. When conducting verification at the time of a transaction, business operators might not be able to detect whether a person is pretending to be another if non-photographic ID is used for customer identification documents.

Therefore, it is recognized that non-photographic ID is vulnerable to misuse for ML/TF, and that transactions with customers who present non-photographic ID present higher risks than transactions using photographic ID.

Moreover, in the Third Round Mutual Evaluation of Japan by the FATF, it was pointed out that when documents not accompanied by photographs are used for customer identification, additional secondary measures should be taken.

○ Measures to contribute to mitigating risks

In light of the abovementioned risks and the matters pointed out by the FATF, revision of the Act on Prevention of Transfer of Criminal Proceeds of 2014 and the accompanying revision of the Enforcement Order and the Ordinance specify the following measures as the methods for identifying specific persons when customers submit non-photographic ID: (1) not unnecessarily sending documents related to the transactions to the residence written on the relevant identification document by registered mail that requires no forwarding; (2) requiring other identification documents or supplementary documents to be submitted when using certain certificates without a photograph (which is issued only once, such as a health insurance card; the same applies to (3)); and (3) requiring other identification documents or copies thereof, or supplementary documents or copies thereof, to be submitted when using certain identification documents without a photograph. These revisions took effect on October 1, 2016.

○ Present Risk

It is recognized that as a result of the abovementioned revisions, the difference in the degree of risk between the customer identification method using photographic ID and the customer identification method using non-photographic ID has decreased. In addition, efforts are being made to raise awareness about the specifics of the revisions among specified business operators.

As a result, although the 2015 and 2016 National Risk Assessment-Baseline Analysis Reports assessed that transactions with customers presenting non-photographic ID present a higher risk than transactions using photographic ID, it is recognized that the risk level has declined.

On the other hand, given that non-photographic ID is still less reliable than photographic ID, it is necessary to identify customers in accordance with the Act on Prevention of Transfer of Criminal Proceeds and to continue focusing on cases where customers deliberately refuse to present photographic ID as cases that present a risk of misuse for ML/TF.

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 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) Specified 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)

Conclusion, etc. of insurance contracts including each transaction prescribed in Article 4, paragraph 1, item 2 of the Ordinance ((a) Insurance contracts without payment of maturity insurance money etc.; (b) Insurance contracts for which total repayment is under 80% of the total premium), falls under the transactions with factors to 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.

(6) Specified 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.

---

*1 In the Act on Prevention of Transfer of Criminal Proceeds and the Enforcement Order, any transactions for which simplified CDD is permitted, prescribed by the Ordinance are excluded from specified transactions that require verification at the time of transaction. However, these are not excluded from specified business that require preparing and storing transaction records and reporting suspicious transactions -- they are subject to prescribed CDD. In addition, the law stipulates that if the transaction is suspicious or is one that requires special attention in CDD, then such transaction is added to specified transactions and subject to verification at the time of transaction, even if the transaction would normally be permitted simplified CDD for.

*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.

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) Specified 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, (f) of the Ordinance, falls under transactions with factors to mitigate risks (vii) and (viii). Therefore, they are deemed to present a low risk.

(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 so-called special account[*2] 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.

---

*1 Individual credit is a form 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. Incidentally, a tie-up loan is a kind of individual credit. There are tie-up loans in which financial institutions and sellers cooperate to provide funds for sales contracts or service provision contracts and tie-up loans that purchasers apply to individual credit operators. Business operators examine and consent, and financial institutions lend funds to the purchasers on condition that the individual credit operators guarantee the loan.

*2 An account opened in a trust bank by a company issuing shares when the company cannot know the accounts of shareholders.

(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 International Transactions in Section 4. High-Risk Transactions, 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) Specified Transactions in Telephone Receiving Service Contracts (Article 4, paragraph 1, item 12 of the Ordinance)

Specified transactions in telephone receiving services, including transactions prescribed in Article 4, paragraph 1, item 12 of the Ordinance ((a) a service contract for a telephone receiving service in which indicating that being a telephone receiving service provider to a third party is included, (b) a contract for a call center business etc.[*2]), fall under transactions with factors to 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.

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.

(14) Specified Transactions in Agent Work, etc. for Specified Mandated Acts by a Judicial Scrivener etc.[*3] (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.

---

*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.

*3 Regarding agent work, etc. for specified mandated acts pertaining to the management or disposition of property listed in item 3 of the middle column of the row of persons listed in Article 2, paragraph 2, item 44 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.

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.