Tentative Translation

December 2018

National Risk Assessment of Money Laundering and Terrorist Financing

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 Crimes	Act on Punishment of Organized Crimes and Control of Crime Proceeds (Act No. 136 of 1999)
Act on Punishment of Terrorist Financing	Act on Punishment of Financing to Offences of Public Intimidation (Act No. 67 of 2002)
Criminal Proceeds Act	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)
Ordinance	Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds (Ordinance of the Cabinet Office, Ministry of Internal Affairs and Communications, Ministry of Justice, Ministry of Finance, Ministry of Health, Labour and Welfare, Ministry of Agriculture, Forestry and Fisheries, Ministry of Economy, Trade and Industry, and Ministry of Land, Infrastructure, Transport and Tourism No. 1 of 2008)
Amusement Business Act	Act on Control and Improvement of Amusement Business, etc. (Act No. 122 of 1948)
Anti-Boryokudan Act	Act on Prevention of Unjust Acts by Organized Crime Group Members (Act No. 77 of 1991)
Anti-Drug Special Provisions Act	Act on Special Measures for the Narcotics and Psychotropics Control Act, etc. and Other Matters for the Prevention of Activities Encouraging Illicit Conduct and Other Activities Involving Controlled Substances through International Cooperation (Act No. 94 of 1991)
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)

Section 1. Overview of Risk Assessment ····· 1
1. Background ····· 1
2. Purpose ····· 1
3. Assessment Methods ····· 4
(1) FATF Guidance ····· 4
(2) This Risk Assessment ····· 4
4. Main Contents ····· 5
(1) Main Assessment Findings from Preceding Years ····· 5
(2) Main Assessment Findings of This Year ····· 7
Section 2. Analysis of Money Laundering Cases, etc. ····· 11
1. Offenders ····· 11
(1) Boryokudan ····· 11
(2) Foreigners in Japan ····· 11
(3) Specialized Fraud Group etc. ····· 12
2. Modus Operandi ····· 12
(1) Predicate Offenses ····· 12
(2) Major Transactions etc. Misused for Money Laundering ····· 17
Section 3. Risk of Products and Services ····· 19
1. Major Products and Services in which Risk is Recognized ····· 19
(1) Products and Services Dealt with by Deposit-taking Institutions ····· 19
(2) Insurance Dealt with by Insurance Companies, etc. ····· 29
(3) Investment Dealt with by Financial Instruments Business Operators and Commodity Derivatives Business Operators ····· 32
(4) Trust Dealt with by Trust Companies etc. ····· 36
(5) Money Lending Dealt with by Money Lenders etc. ····· 38
(6) Funds Transfer Service Dealt with by Funds Transfer Service Providers ····· 40
(7) Virtual Currency Dealt with by Virtual Currency Exchange Service Providers ····· 44
(8) Foreign Currency Exchange Dealt with by Currency Exchange Operators ····· 48
(9) Financial Leasing Dealt with by Financial Leasing Operators ····· 52
(10) Credit Cards Dealt with by Credit Card Operators ····· 54
(11) Real Estate Dealt with by Real Estate Brokers ····· 57
(12) Precious Metals and Stones Dealt with by Dealers in Precious Metals and Stones ····· 60
(13) Postal Receiving Service Dealt with by Postal Receiving Service Providers ····· 64
(14) Telephone Receiving Service Dealt with by Telephone Receiving Service Providers ····· 67
(15) Telephone Forwarding Service Dealt with by Telephone Forwarding Service Providers ····· 68
(16) Legal/Accounting Service Dealt with by Legal/Accounting Professions ····· 70
2. Products and Services Utilizing New Technology, Which Requires Further Examination of Actual State of Use etc. (Electronic Money) ····· 73
Section 4. High Risk Transactions ····· 76
1. Transaction Type ····· 76
(1) Non-face-to-face Transactions ····· 76
(2) Cash Transactions ····· 79
(3) International Transactions ····· 81
2. Countries/Regions ····· 85
3. Customer Type ····· 88
(1) Anti-social Forces (Boryokudan etc.) ····· 88
(2) International Terrorists (Such as Islamic Extremists) ····· 90

(3) Non-resident Customers……95
(4) Foreign Politically Exposed Persons……96
(5) Legal Persons without Transparency of Beneficial Ownership……98
Section 5. Low Risk Transactions……102
1. Factors to Mitigate Risks…… 102
2. Low Risk Transactions …… 103
(1) Specified Transactions in Money Trusts, etc. (Article 4, paragraph 1, item 1 of Ordinance)· 103
(2) Conclusion etc. of Insurance Contracts (Article 4, paragraph 1, item 2 of Ordinance) …… 103
(3) Payment of Maturity Insurance Money etc. (Article 4, paragraph 1, item 3 of Ordinance) … 103
(4) Transactions Carried out on a Securities Market etc.
(Article 4, paragraph 1, item 4 of Ordinance) …… 103
(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 Ordinance)…… 103
(6) Specified Transactions Concerning Loan of Money etc.
(Article 4, paragraph 1, item 6 of Ordinance) …… 103
(7) Specified Transactions in Cash Transactions etc.
(Article 4, paragraph 1, item 7 of Ordinance) …… 104
(8) Opening a Special Account under the Act on Transfer of Bonds, Shares, etc.
(Article 4, paragraph 1, item 8 of Ordinance) …… 104
(9) Transactions through SWIFT (Article 4, paragraph 1, item 9 of the Ordinance) …… 105
(10) Specified Transactions in Financial Leasing Contracts
(Article 4, paragraph 1, item 10 of Ordinance)…… 105
(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 Ordinance)…… 105
(12) Specified Transactions in Telephone Receiving Service Contracts
(Article 4, paragraph 1, item 12 of Ordinance)…… 105
(13) Transactions with the State etc. (Article 4, paragraph 1, item 13 of Ordinance)…… 105
(14) Specified Transactions in Agent Work etc. for Specified Mandated Acts by a Judicial Scrivener etc. (Article 4, paragraph 3 of Ordinance)…… 105

Section 1. Overview of Risk Assessment

1. Background

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

In the new "40 Recommendations"[*2] revised in February 2012, the Financial Action Task Force (FATF)[*3] 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 new "40 Recommendations" of the FATF 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 of Money Laundering and Terrorist Financing" (hereinafter referred to as "Assessment Report") was published.

Since then, pursuant to the provisions of Article 3, paragraph 3 of the Criminal Proceeds Act[*4], which were newly established when the act was revised in 2014, the National Public Safety Commission has prepared and published an annual national risk assessment of money laundering and terrorist financing (hereinafter referred to as "assessment report"), which describes risks, etc. in each category of the transactions carried out by business operators, in keeping with the contents of the Assessment Report.[*5]

2. Purpose

FATF 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 for their products and services" to implement the risk-based approach. In order for specified business operators in Japan to accurately determine whether there are transactions suspicious of ML/TF within the huge number of transactions that are undertaken, it is more effective to rely on methods which adopt the risk-based approach, like checking high risk transactions more rigorously than usual transactions, instead of conducting an across-the-board examination of all transaction records. 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

---

*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 making an arrest. In Japan, money laundering is prescribed as an offence in the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Act.

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

*3 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.

*4 The Article provides that the "National Public Safety Commission shall each year conduct investigation and analysis on the modus operandi and other circumstances of the transfer of criminal proceeds to prepare and publish a national risk assessment of money laundering and terrorist financing, 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 which require attention as remittance destinations may be different between money laundering and terrorist financing. The present assessment report 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 assessment report include terrorist financing risks.

position to gather, arrange, and analyze information relating to the transfer of criminal proceeds or concerning suspicious transactions, is to prepare and publish an assessment report describing risks for each category of transactions carried out by business operators. Expert knowledge and information are to be obtained from administrative authorities supervising specified business operators (hereinafter referred to as "competent administrative 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 Criminal Proceeds Act, which stipulates the methods for making dicisions about reporting suspicious transaction 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 assessment report, in addition to the Order and Ordinance for Enforcement of the revised Act.

Specified business operators are required to implement appropriate measures based on the abovementioned revised Act, in order to prevent the transactions they handle from being misused for ML/TF. Specifically, specified business operators are required to consider the contents of the assessment report (Section1to4) relating to the transactions they handle, etc.. They also need to keep in mind the reasons why those transactions are considered risks or high risks 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 assessment report but also the contents of guidelines by the competent administrative authorities. When the counterparty to the transaction is a specified business operator, it is also considered useful to look at factors affecting the risks and the status of the AML/CFT systems, relating to the products and services handled by the counterparty, described in the assessment report.

Moreover, the Criminal Proceeds Act and the Ordinance call on specified business operators to apply the risk-based approach based on the risk assessment performed in this manner, in order to accurately perform verification at the time of transaction commensurate with the risk level of their own transactions. Legal obligations for accurately performing verification at the time of transaction are shown below.

[Legal Obligations Imposed on Specified Business Operators and Their Offences]

The Criminal Proceeds Act and its Enforcement Order and Ordinance oblige specified business operators to perform verification at the time of specified transactions, prepare and keep verification records, etc., 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. The Act also provides that in so far as necessary for the enforcement of the Act, competent administrative 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 administrative authorities and conduct inquires necessary for this purpose. It furthermore stipulates penalties for violations of rectification orders.
Between 2015 and 2017, six rectification orders were issued under the Act (see table 1), mainly concerning offences related to verification at the time of transaction and the preparation and keeping of verification records. Regarding these offences, competent administrative authorities ordered specified business operators to take the following rectification measures within fixed periods of time:

○ Reaffirming provisions of the Act on Prevention of Transfer of Criminal Proceeds through in-house education, etc.
○ Developing manuals to smoothly proceed with measures 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 signed contracts in the past, and prepare and keep verification records

In addition, specific violations found through reports collected from specified business operators by the National Public Safety Commission in 2017 are as follows:

○ Neglected to verify the customers' purposes of transactions, their occupations, etc.
○ Neglected to verify the beneficial ownership and corporate customers
○ Neglected to send transaction documents by registered mail of no-forwarding in non-face-to-face transactions
○ Neglected to prepare or keep verification records

Table 1 [Numbers of Reports Collected by National Public Safety Commission/National Police Agency, etc. and of Rectification Orders Issued by Competent Administrative

Authorities Receiving Statements of Opinion]

Category \ Year	2015	2016	2017
Number fo requests to submit reports to specified business operators	11	9	7
Number of directions to conduct inquiry to prefectural police	2	0	0
Number of opinion statements made to competent administrative authorities	10	8	7
Number of rectification orders based on opinion statements	5	0	1

[Risk Control by Business Operators (Developing Internal Systems Based on the Risk-based Approach)]
Regarding the abovementioned offences, some cases were identified in which internal control rules for accurately performing verification at the time of transaction, etc. were not developed, in which persons responsible for verification at the time of transaction, etc. did not understand laws or regulations, etc., requiring specified business operators to improve their systems for accurately performing verification at the time of transaction, etc. Given these findings, the revised Criminal Proceeds Act and its Enforcement Order and Ordinance, put into effect on October 1, 2016, 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 audit 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 assessment report, as prescribed by the Ordinance

The Ordinance prescribes the following measures:

○ Implement specified business operators' own risk assessment (including the preparation of a written Risk Assessment Report by a Specified Business Operator, 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 for accurate implementation of measures, including verification at the time of transaction
○ Conduct audits required to accurately implement measures, including verification at the time of transaction

(*) The following are high-risk transactions:

○ Transactions prescribed in the first sentence of paragraph 2 of Article 4 of the Criminal Proceeds Act (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 (hereinafter referred to as "specific countries, etc."), 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 manners 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 assessment report
○ Transactions that are deemed high ML/TF risks in light of the contents of the assessment report

3. Assessment Methods

(1) FATF Guidance

For risk assessment methods, we referred 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, the Guidance shows risk factors and an evaluation process an general:

A. Risk Factors

Risk can be assessed by 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 effect on the reputation and attractiveness of a country's financial sector, etc.

B. Evaluation Process

The evaluation 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)
  Consider the nature, likelihood, etc. of the identified risks or risk factors.
- ○ Evaluation process (stage III)
  Determine priorities for addressing the risks.

(2) This Risk Assessment

A. Assessment Method

In this risk assessment, in light of the Guidance, we referred to the new "40 Recommendations" of the FATF and its Interpretive Notes[*1], the measures under the Criminal Proceeds Act, the matters pointed out in the Third Round Mutual Evaluation of Japan conducted by the FATF[*2], and the cleared cases of money laundering offences, in order to consider the following in Japan:

- ○ Threat
  Offenders including Boryokudan (Japanese organized crime groups), foreigners in Japan, specialized fraud groups, etc. and predicate offences, etc. including theft, fraud, etc.
- ○ Vulnerability
  Products/services including deposit/savings accounts, domestic exchange transactions, etc. and transaction types, etc. including non-face-to-face transactions, cash transactions, etc.

---

*1 As examples of situations that increase the ML/TF risks, the Interpretive Note to Recommendation 10 (Customer Due Diligence) cites "non-resident customers," "legal persons or legal arrangements that are personal asset-holding vehicles", "business that are cash-intensive", "the ownership structure of the company that appears unusual or excessively complex", "countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems", "non-face-to-face business relationships or transactions", etc.

*2 In the Third Round Mutual Evaluation of Japan conducted by the FATF, it has been pointed out that "in case customer identification documents do not include photographic identification, additional secondary measures should be taken", "when the customer is a legal person or legal arrangement, the natural person who ultimately owns or controls the legal person or legal arrangement should be identified, in order to understand the beneficial ownership and control of the customer", "when the customer is a foreign politically exposed person (PEP), specific steps should be taken, in addition to regular CDD measures," "the identification and verification requirements for non-face-to-face transactions are insufficient", etc. As a side note, on October 1, 2016, risk mitigation measures were taken under the Criminal Proceeds Act.

○ Consequence
Amounts of criminal proceeds to be transferred, risks of supporting or facilitating organized crimes, impact on sound economic activities, etc.
Subsequently, we identified risk factors[*1] in terms of "products/services," "transaction types," "countries/regions," and "customer attributes."
Then, we analyzed the following for each risk factor, in order to make a multilateral and comprehensive evaluation of risks:
○ Inherent risks of being misused for ML/TF
○ Status of STRs
○ Money laundering offences
○ Status of the risk mitigation measures in place (including legal obligations imposed on business operators, guidance/supervision for business operators by competent administrative authorities, voluntary measures by industry groups or business operators).

B. Information Used in the Assessment

For the assessment, in addition to statistics, case examples, etc. held by relevant ministries and agencies, we used extensive amounts of information collected through the relevant ministries and agencies on the products/services handled by industry groups or business operators, the types, scale, 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 to the above information, we used information on money laundering offences cleared and STRs, mainly during the past three years (2015–2017), etc.

4. Main Contents

(1) Main Assessment Findings from Preceding Years

ML/TF risks surrounding Japan are always changing, and the assessment reports that have been prepared every year from 2015 contain the contents that correspond to these changes.

In the previous Assessment Report, the range of products/services considered to have risks are limited but in the 2015 assessment report, the range of products/services was expanded to include all transactions carried out by specified business operators under the Criminal Proceeds Act, and analysis and evaluation were performed on the range of products/services.

In the 2016 assessment report, "Virtual Currency dealt with by Virtual Currency Exchange Service Providers" were added to the products/services considered to have risks, and "International Terrorists (Islamic Extremist Groups, etc.)" to the customers who make high-risk transactions. Virtual currency was described as "Products/Services Utilizing New Technology Which Requires Further Examination of Actual State of Use etc" in the 2015 assessment report, but in light of what has been pointed out internationally, their actual usage, etc. since then, deeper assessment and analysis were performed on the ML/TF risks of virtual currency, leading to their addition to the products/services considered to have risks. In addition, while no independent analysis was added on terrorist financing in the 2015 assessment report, in consideration of the situation, etc. requiring stronger CFT measures against ISIL, AQ, etc. at the international level, a dedicated analysis was carried out on international terrorists in the 2016 assessment report. The report focused on differences between money laundering and terrorist financing ((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 which require attention as remittance destinations may be different between money laundering and terrorist financing), etc.

In the 2017 assessment report, in light of the fact that the smuggling of gold bullion is on the increase in Japan, the results of analysis on the factors that increase the risks, including the highly anonymous, predominantly cash-based transactions of gold bullion, in addition to the manner of crimes and the characteristics of the countries/regions of origin, were added to the item "Precious Metals and Stones

*1 In addition to them, factors that increase the risks include the scales of business operators. As the number and volume of transactions increase, it becomes more difficult to identify and trace criminal proceeds in the transactions, and because of this, among other reasons, larger business operators are generally considered to present higher risks. In response, the Criminal Proceeds Act requires business operators to strive to develop necessary systems, including implementation of 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.

Dealt with by Dealers in Precious Metals and Stones". Likewise, in response to organized, cross-border money laundering offences, analysis results on the factors that increase the risks, including the type of crime and the trend of international criminal organizations, were added to the item "International Transactions."In addition, transactions using identification documents without photographs were formerly considered higher risks than those using identification documents with photographs, due to the inferior ability of such documents to prove identity, etc., compared to identification documents with photographs. But given that, the revised Criminal Proceeds Act and its Enforcement Order and Ordinance were put into effect on October 1, 2016 in response to the risks to require taking appropriate additional measures in cases of transactions with customers, etc., who present an identification document without a photograph, "Transactions with Customers Who Use an Identification Document without a Photograph" was excluded from high-risk transactions.

Revisions to the Criminal Proceeds Act and its Enforcement Order and Ordinance in accordance with the ML/TF risks are shown below.

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

The present assessment report identifies ML/TF risk factors in terms of "products/services", "transaction types", "countries/regions", and "customer attributes", taking into account the new "40 Recommendations" of the FATF, the matters pointed out in the Third Mutual Evaluation of Japan conducted by the FATF, the modus operandi of money laundering offences identified, etc.

In light of these factors, etc., as a risk mitigation measure, Japan has revised the Criminal Proceeds Act and its Enforcement Order and Ordinance to impose stricter obligations on business operators.
The recent major revisions to the Criminal Proceeds Act, etc. are as follows:

○ Revisions to the Criminal Proceeds Act, etc. put into effect on October 1, 2016

- Clarification of methods for making decisions about suspicious transaction reporting
  Specified business operators (excluding judicial scriveners, etc.) should decide on whether to file STRs, by considering the contents of the assessment report and the methods prescribed by the Ordinance (including a comparison with the mode of ordinary transactions related to the specific business), in addition to the results of the verification at the time of transaction, the modes of the transactions in question, or other circumstances.
- Verification obligation at the time of conclusion of correspondence contracts[*1]
  When specified business operators who carry out exchange transactions on a commercial basis enter into correspondent banking relationships with exchange transaction business operators located in foreign countries, they should verify that these operators abroad have developed systems necessary for accurately implementing the measures equivalent to verification at the time of transaction, etc.
- Implementation of enhanced CDD at the time of transaction with foreign PEPs
  Specified transactions with foreign PEPs should be added to the transactions that are 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 ownership of the legal persons or legal arrangements.
- Customer identification methods involving identification documents without photographs
  When 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 customers' home addresses by the postal item requiring no forwarding.
- Implementation of verification at the time of transaction divided into multiple transactions in order to become below the threshold
  When it is immediately obvious that a single transaction is divided into multiple transactions below the threshold to reduce the transaction amount for each transaction, they should be regarded as a

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

single transaction.

○ Revisions to the Criminal Proceeds Act put into effect on April 1, 2017

Virtual currency exchange service providers are added to specified business operators.

○ Revisions to the Ordinance promulgated on November 30, 2018

To support FinTech, a new mechanism should be established for the completion of online customer identification, and more rigorous identification methods should be applied in case postal mail is used by the postal item requiring no forwarding in non-face-to-face transactions.

(2) Main Assessment Findings of This Year

In order to promote understanding of how criminal proceeds are generated and transferred in transactions handled by business operators, etc., this year's assessment report published the results of the assessment and analysis of the form of crimes, modus operandi of ML/TF pertaining to the predicate offences, etc. In addition, the findings from the expanded analysis, especially of virtual currency, precious metals, telephone forwarding services, legal persons without transparency of beneficial ownership, etc., were included as content reflecting the status of ML/TF risks based on the recent situation.

Moreover, the assessment results of risk mitigation measures for products/services, including not only legal measures but also operational measures, such as the status of activities relating to risk assessment and risk-based approach performed by competent administrative authorities and specified business operators, were also published in the assessment report.

General summery of these points are as follows.

As matters now stand, competent administrative authorities develop guidelines, taking into account the contents of the assessment report. They then call on specified business operators to build and maintain ML/TF risk control systems, and survey these operators about their compliance with laws and regulations, including the Criminal Proceeds Act, their implementation of risk assessment and the risk-based approach that is based on it, etc. Then, using the information obtained this way, competent administrative authorities identify and assess the risks associated with business categories or business operators under the jurisdiction, in order to promote guidance/supervision, etc. commensurate with the risks.

Specific measures against the risks that are being taken include giving greater supervision on deposit-taking financial institutions and fund transfer service providers, which places importance on remittance transactions like overseas remittances, setting up special monitoring teams for virtual currency in order to promote registration screening and on-site inspections concerning Virtual currency exchange service providers, offering thorough administrative guidance on the non-fulfillment of obligations or a lack of understanding of obligations to the dealers in precious metals, etc.

Specified business operators are also promoting AML/CFT systems or controls through their activities related to risk assessment and the risk-based approach.

For example, taking into account the assessment report, guidelines by competent administrative authorities, etc., some operators conduct comprehensive and concrete studies of their products/services, the geographical features of their business territories, etc. to identify risks, and build effective control systems at the organizational level under the involvement of the management. Specific activities of business operators are described individually in "Section 3. Risks of Products and Services," but they are also listed below in order to be understood at a glance.

However, as matters now stand, there are disparities in the activities by business category or business operator, and, in some situation, it has been recognized that the more the scale of operations of the business operator becomes smaller, the less the implementation of the AML/CFT measures.

In contrast, regarding the relationship between the scale of operations and the risks, generally, the more the scale of operations becomes, the more difficult it becomes to identify and trace criminal proceeds in the operations, and that results in increased risks. However, competent administrative authorities and business operators need to keep in mind that if the contents of the products/services being handled are the same, the inherent risks of being misused for ML/TF do not vary greatly with the scale of operations.

Even if some business categories or business operators adopt substantive AML/CFT systems based on the risk-based approach, if there remain business categories or business operators that take only

insufficient superficial measures without allocating necessary resources, those who attempt to commit ML/TF will engage in ML/TF through those business categories or business operators that take only half measures, and ultimately ML/TF cannot be effectively controlled. Thus, in order to effectively deter ML/TF, it is essential that all business categories and business operators promote substantive measures based on individual risks.

Competent administrative authorities are required 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 the jurisdiction. Furthermore, it is not only necessary to provide appropriate guidance/supervision, including administrative guidance, to business operators who do not very actively engage in the activities, but also to share information necessary for the activities, countermeasures cases, etc. with such business operators, in collaboration with industry groups, etc., in order to raise the level of AML/CFT systems of the whole business category.

It goes without saying that business operators need to thoroughly fulfill their legal obligations, but they need to go beyond verifying whether they have committed any violations of laws, regulations, etc. as a matter of formality. They will need to comprehensively and specifically estimate their business characteristics and the risks involved, identify the risks they face, and give substantive responses.

In addition, a constant review of the occasionally changing ML/TF situations using the risk assessment and risk-based approach, shared between the public and private sectors, is necessary for continuously carrying out such activities.

The importance of risk assessment and risk-based approach based on it is being communicated by competent administrative authorities to business operators through guidance and supervision, the organization of workshops, etc.

Moreover, information about the abovementioned activities is also being communicated to the public through the websites of the Government Public Relations and the Financial Services Agency, newspapers, etc.. Because it is essential to promote understanding and cooperation of the public, who uses business operators, in order to implement appropriate CDD, etc. Through these measures and policies, Japan promotes the understanding of the ML/TF risks and the risk-based approach that is based on them to further enhance the AML/CFT systems or controls.

[Cases of risk assessment and risk-based approach performed by specified business operators]

[Deposit-taking financial institutions]

○ Cases where a company analyzes suspicious transactions reported by the company and extracts an independent risk index from the tendency of countries and areas of destination and origin regarding overseas transfer, tendency of nationality regarding accounts by names of foreigners and tendency of occupation or type of business regarding customers.

○ Cases where a company, not only taking direct description in the assessment report into account, but also by taking into account the principle of the description, identifies specific risks where foreigners who assume their return 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 concentrated manner may receive a mixture of unauthorized funds in transactions.

○ Since transaction achievement of goods, customer types, geographical characteristics and so on vary according to branch offices, each branch office analyzes independently focusing goods and services, transaction type, country and area, attributes of customers.

○ Cases where the length of visa of customers who are foreign workers or students is checked and controlled by a system for the risk of sale of accounts at the time of their return.

○ Cases of banks which have an internal regulation in which accounts which are opened by a small amount, accounts of persons who live in a remote area, or accounts of corporations which are incorporated and relocated just before and so on are designated as the control subject accounts and, if any request for transfer to such accounts occurs, the consistency of such request with the purpose of opening the account is checked and the intent of a person requesting the transfer is checked, and, if the consistency cannot confirmed, the transaction is denied or the report of suspicious transaction is made.

[Foreign currency exchange business operators]

○ Cases where transactions for certain amount are classified into high-risk transactions and, if such transactions occur, measures such as report to the headquarter and execution of necessary research are specified in internal regulations.

○ Cases where, considering risks in which large transactions are intentionally separated into more than one small transaction for the purpose of getting off the verification at the time of transaction, the verification at the time of transaction is conducted based on a threshold value which is independently specified internally, and results are made into a database, and the existence of customers who conduct transactions of a large amount in the total amount is monitored.

[Credit card operators]

○ Case 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, credit card function is suspended, and a telephone call is given to a card holder to check the content of use or the user.

○ A case where the increase of the availability of a credit card is not authorized in principle until one year elapses after the application to mitigate risks by a person attempting money laundering using a contract is mitigated.

[Real Estate Brokers]

○ A case where information on transactions with customers for whom transactions were cancelled or transactions were not achieved for any reason in the past is made into a database to share by all employees of the company and, if any subsequent transactions with such customers occur, measures to strengthen customer control or to reject transactions are taken.

○ A case where, in order not to overlook transactions with Anti-social Forces, an operator independently prepares a checklist regarding characteristics of speech and behavior of Anti-social Forces and utilize the checklist for customer control.

[List of Main Contents of the 2018 Assessment Report]
(Content mainly added, etc. this year, compared to last year, are marked with * in the table)

Analysis of money laundering offences, etc.		(1) Offenders (Boryokudan, foreigners in Japan, specialized fraud groups, etc.) (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 the purpose of gain, violation of the Amusement Business Act, violation of the Anti-Prostitution Act) * Description of the analysis results on the modus operandi of ML/TF. for each predicate offence
High Risk Transactions	Transaction types	(1) Non-face-to-face Transactions * Description of content that reflect the revision to the Ordinance, which introduced a mechanism for online completion (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 (in the 2015 assessment report, Algeria and Myanmar were listed, in addition to those countries)) * Description of the trends in the FATF Public Statement over the past three years
	Customer attributes	(1) Anti-social Forces (Boryokudan, etc.) (2) International Terrorists (Islamic Extremist Groups, etc.) (added in the 2016 assessment report) (3) Non-resident Customers (4) Foreign Politically Exposed Persons (5) Legal Persons without Transparency of Beneficial Ownership * Especially, addition of analysis results, etc. on cases of misuse by legal persons without transparency of beneficial ownership ("Transactions with Customers Who Use an Identification Document without a Photograph" was excluded from the 2017 assessment report)
Products/services considered to have risks		(1) Products/Services Dealt with by Deposit-taking Financial Institutions (deposit/savings accounts, deposit transactions, domestic exchange transactions, safe-deposit boxes, notes/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) Virtual Currency Dealt with by Virtual Currency Exchange Service Providers (added in the 2016 assessment report) (8) Foreign Currency Exchanges Dealt with by Currency Exchange Business 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 Service Dealt with by Postal Receiving Service Providers (14) Telephone Receiving Service Dealt with by Telephone Receiving Service Providers (15) Telephone Forwarding Service Dealt with by Telephone Forwarding Service Providers (16) Legal/Accounting Service Dealt with by Legal/Accounting Professions * Especially, addition of virtual currency, precious metals, call forwarding services, etc.
Low Risk Transactions	Factor	(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. by 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 allowing simple CDD, prescribed in Article 4 of the Ordinance (note, however, that simple CDD is not allowed in the case of suspicious transactions, etc.)
Products/services using new technology		Electronic money

Section 2. Analysis of Money Laundering Cases, etc.

1. Offenders

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

(1) Boryokudan

In Japan, money laundering by Boryokudan is especially a serious threat. Among cleared money laundering cases in 2017, 50 cases (13.9%) were related to Boryokudan members, associates and other related parties (hereinafter referred to as "Boryokudan gangsters") (see table 2). Out of those 50, 46 cases fell under the Act on Punishment of Organized Crimes, Control of Crime Proceeds and Other Matters (22 for concealment of criminal proceeds and 24 for receipt of criminal proceeds) and four fell under the Anti-Drug Special Provisions Law (three for concealment of illegal drug proceeds and one for receipt of illegal drug proceeds).

In addition, in the last three years, the majority of cleared cases related to Boryokudan gangsters are fraud and theft. On the other hand, regarding the number of Boryokudan gangsters as a proportion of arrested offenders, they were deeply involved in loan shark, gambling, and prostitution offenses.

Boryokudan repeat crimes professionally to gain economic profit and carry out money laundering tactically.

Money laundering by Boryokudan seems to be carried out internationally, and the U.S. published "Strategy to Combat Transnational Organized Crime" and enacted a Presidential decree in July 2011. In them, the U.S. designated Boryokudan gangsters of Japan as one of "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 the citizens from dealing with Boryokudan gangsters.

With respect to Boryokudan, the results of survey and analysis are also explained in the item "Anti-social Forces (Boryokudan, etc.)" in "Section 4. High Risk Transactions" of this report.

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 (2015–2017)]

Category \ Year	2015	2016	2017
Cleared cases of money laundering offenses	389	388	361
Cases by Boryokudan gangsters	94	76	50
Percent (%)	24.2%	19.6%	13.9%

(2) Foreigners in Japan

Of cleared money laundering cases in 2017, 27 cases (7.5%) were committed by foreigners in Japan (see table 3). The breakdown comprised was 20 cases for concealment of criminal proceeds and seven cases for receipt of criminal proceeds.

In the cleared money laundering cases under the Act on Punishment of Organized Crimes in the last three years, China, Vietnam and Nigeria are in this order top 3 countries where arrested offenders are from. China occupies more than half of the total. 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 by illegal access 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, China and Philippines lead the rankings of numbers of cleared offenses 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.And increase in the number of cleared offenses by Vietnamese has been noticeable in recent years.

Furthermore, with respect to the number of STRs in the last three years, STRs related to China, Vietnam, and Korea are top 3 in numbers, and there is a remarkable increase in reports related to Vietnam in these days.

Criminal proceeds from offenses in which foreigners in Japan are involved are difficult to trace. This is

because there are different legal and transactions systems surrounding the transfer of criminal proceeds across the border.

With respect to international transactions, "International Transactions" in "Section 4. High Risk Transactions" of this report also explain the results of surveys and analysis.

Table 3 [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 (2015–2017)]

Category \ Year	2015	2016	2017
Cleared cases of money laundering offenses	389	388	361
Cases by foreigners	34	35	27
Percent (%)	8.7%	9.0%	7.5%

(3) Specialized Fraud Group etc.

Japan has recently witnessed a rise in specialized fraud cases. Offenders deceives victims without actually meeting them by phone calls and other means and swindle them out of money.[*1] Having the ringleader as the core, specialized fraud groups set each role. For example, one member cheats victims, another draws money, and the other procures a crime tool. In this way, they commit organized fraud. In addition, they commit money laundering, for example, by using bank accounts in the name of fictitious or another party as a tool to receive money from a victim (see table 4).

Furthermore, there are some people who thoughtlessly sell their own bank account to get their amusement expenses or the cost of living. Some even make bank accounts in the name of fictitious or another party by using a falsified ID card and sell them. Such people make money laundering easier.

Table 4 [Number of Specialized Fraud cases recognized and Total Financial Damage (2015–2017)]

Category \ Year	2015	2016	2017
Number of recognized cases	13,824	14,154	18,212
Total financial damage (yen) (Effective total amount of financial damage)	48,197,981,078	40,765,652,881	39,474,870,491

Note 1: Data from the National Police Agency
2: Effective total amount of financial damage means original damage from fraud plus money which was withdrawn (stolen) from ATMs by the use of defrauded cash cards.

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 business operation of companies by using such proceeds. In June 2017, the Act on Punishment of Organized Crimes was revised to substantially increase the predicate offenses. They include offences which generate illegal proceeds and subjected to the death penalty, or life or four-year or longer imprisonment with or 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 subjected to the Interest Deposit and Interest Rate 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.

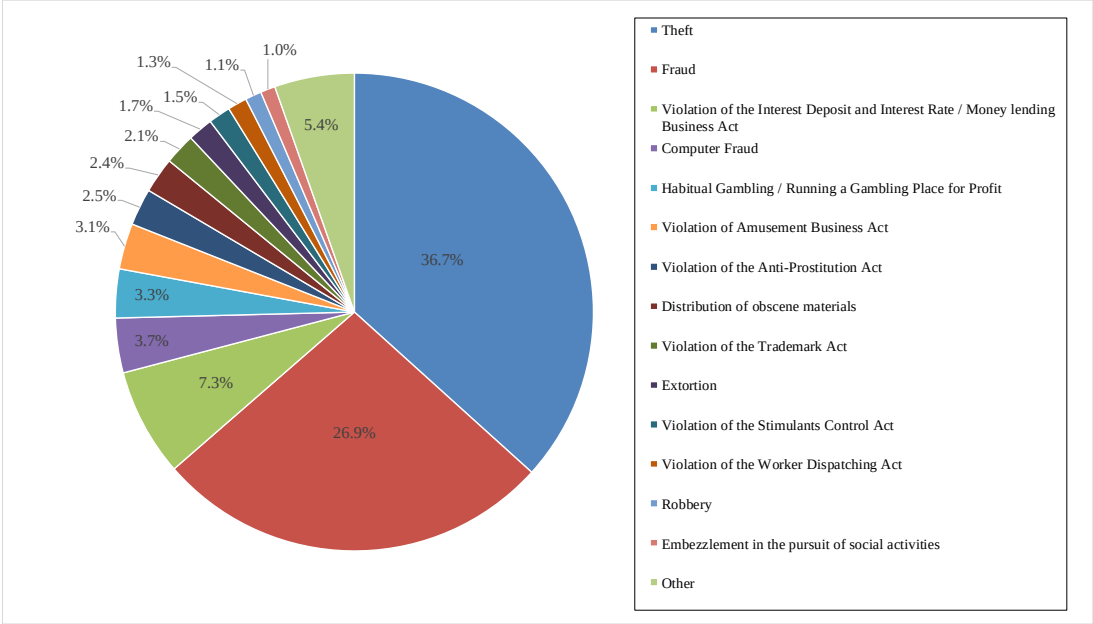
Among cleared money-laundering cases categorized by predicate offenses in 2015-2017[*2], theft was the

*1 Specialized fraud is a collective name of frauds (including extorting money by fraud) where offenders cheat randomly targeted people in a non-face-to-face manner through telephone etc. and making them give money/goods in some way such as payment into designated bank accounts. Specialized fraud includes remittance call fraud, fraud disguising as a financial instruments transaction, fraud disguising as a successful gambling strategies provider, and fraud disguising as a dating agency, etc.

*2 There were 1,138 cleared cases of money laundering under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law from 2015 to 2017. On the other hand, the total number of cleared money-laundering cases counted by predicate offenses was 1,143 (See table 5) because some money-laundering cases can be counted in multiple predicate offenses.

leading crime with 419 cases, accounting for 36.7%, followed by fraud (308 for 26.9%), violation of the Interest Deposit and Interest Rate Act/Money Lending Business Act (Act No. 32 of 1983) (83 cases for 7.3%), computer fraud (42 cases for 3.7%), and habitual gambling/running a gambling place for the purpose of gain (38 cases for 3.3%) (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 (2015–2017)]



Predicate offenses	Theft	Fraud	Violation of the Interest Deposit and Interest Rate / Money lending Business Act	Computer Fraud	Habitual Gambling / Running a Gambling Place for Profit	Violation of Amusement Business Act	Violation of the Anti-Prostitution Act	Distribution of obscene materials	Violation of the Trademark Act	Extortion	Violation of the Stimulants Control Act	Violation of the Worker Dispatching Act	Robbery	Embezzlement in the pursuit of social activities	Others	Total
Total	419	308	83	42	38	35	29	27	24	19	17	15	13	12	62	1143
Ratio (%)	36.7	26.9	7.3	3.7	3.3	3.1	2.5	2.4	2.1	1.7	1.5	1.3	1.1	1.0	5.4	100

The size of generated criminal proceeds, relevance to money-laundering offenses, etc., types of misused transactions, danger of fomenting organized crimes, 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. There are cases in which the amount of damage is comparatively small, but there are also cases committed professionally and repeatedly by crime organizations such as Boryokudan and groups of foreigners in Japan that result in large amounts of criminal proceeds.

For example, there was a case in which 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. Among shoplifting offenses, which comprise the major portion of offenses by Vietnamese (increasing in recent years), there are cases in which acts of stealing, and subsequent reselling activities, etc. are committed in a planned and organized way. In reselling the stolen goods, goods are bought from remote places via parcel delivery service and payments are made by bank transfer in certain cases. Regarding organized car theft committed by Boryokudan and groups of foreigners in Japan, there were cases in which stolen cars were carried to so-called yards surrounded by iron walls, disassembled and then illegally exported overseas.

Among property offenses (robbery with violence, blackmail, theft, fraud, embezzlement and theft of lost or mislaid property) in 2017, the amount of damages was largest for theft, with about 66.7 billion yen (cash damage about 18.2 billion yen) 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 amount of coins obtained via burglary were deposited in 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; and 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.

B. Fraud

(a) Forms of offenses

Fraud offenses, including specialized fraud offenses, have been professionally and systematically committed by domestic and foreign criminal groups. And a large amount of criminal proceeds are generated economic activities desguised to be legitimate such as using bank accounts in the name of fictitious persons or other parties and through transactions by a corporation disguised as if it was 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, and 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.

The total financial damages from fraud offenses in 2017 was about 61 billion yen (cash damage total about 57.1 billion yen). Although the total damages from theft offenses is bigger than that from fraud offenses, the average financial damage due to each fraud case is about 1.43 million yen bigger than that of a theft offense (about 100,000 yen). In particular, specialized fraud offenses generate a large amount of criminal proceeds with an average about 2.29 million yen per case.

(b) Modus operandi of money laundering

Regarding the modus operandi of money-laundering offenses related to fraud as predicate offenses, damages from special fraud offenses are transferred to bank accounts in the name of fictitious or other parties in many cases. 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 in order to circumvent 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, for example, individual persons, corporate bodies, and individual persons accompanied by a "trading-as" name. There are actual cases in which a foreigner in Japan had sold his bank account when leaving Japan and the account was used to receive proceeds of special fraud offenses, a dummy company was incorporated to open deposit accounts for receiving proceeds of special fraud offences, and an account in the name of an individual person accompanied by a "trading-as" 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 criminal organizations committing specialized fraud offenses, etc.

C. Computer fraud

(a) Forms of offenses

Computer fraud are committed to remit the criminal proceeds generated from specialized fraud and illegal internet banking.

One example of this form of specialized fraud is using cash cards cheated from victims to illegally obtain cash by transferring criminal proceeds to the accounts in another party's name via ATM. Damage from this type of offense has been increasing recently.
In terms of illegal remittance offenses related to Internet banking, there were cases where illegal remittances were made from other parties' accounts by illegally accessing the business system managed by financial institutions using ID, password, etc. of other parties. These kind of offence has been generated a large amount of criminal proceeds.The damages in 2017 consisted of 425 cases and the amount exceeded 1 billion yen. While the above offenses have been declining in recent times, illegal remittance offenses by illegal access to virtual currency exchange service providers, etc. has been rising.

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 offenses as predicate offenses, there were case where the maximum amount of cash was withdrawn from ATMs using cash cards obtained via special fraud offenses and the maximum amount for transfer was remitted to accounts in names of other persons. 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 group of Chinese in Japan withdrew cash from the account.

D. Violation of the Interest Deposit and Interest Rate Act/Money Lending Business Act

(a) Forms of offenses

This is a form of loan shark whereby a money lending business operates without a license 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.

A large amount of criminal proceeds were generated. The amount of damages reaches over 9 billion yen, according to the statistics on cleared loan shake black-market lending offenses in 2017. In addition, it is recognized that Boryokudan professionally and systematically operate loan shark as an important source of revenue.

(b) Modus operandi of money laundering

Regarding modus operandi of money-laundering offences related to loan shark as predicate offenses, there have been cases where debt repayments were remmitted 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 a debt repayments from borrowers and illegally used to conceal criminal proceeds.

In addition, there have been cases in which 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 case, loan shark offenders had made borrowers issue drafts and/or checks when borrowing and if there was any delay in repayment, collection is 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 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 cards" 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 revenue for Boryokudan.

In the last three years, the number of cases where restraining order for confiscation by court prior to indictment prescribed by the Act on Punishment of Organized Crimes, Control of Crime Proceeds and Other Matters 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

As modus operandi of money-laundering offences related to habitual gambling/running a gambling place for profit as predicate offenses, there was a gambling offense 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 in which 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 are 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."). Criminak proceeds from amusement-related offenses are an important source of revenue for Boryokudan. There are certain cases in which foreigners living illegally in Japan illegally work 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 restraining order for confiscation prior to indictment as prescribed in the Act on Punishment of Organized Crimes, Control of Crime Proceeds and Other Matters.

(b) Modus operandi of money laundering

As 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 in which sales proceeds paid by credit cards were transferred to a bank account in the name of another party, and 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

The amount of stimulants smuggled into Japan in 2017 and confiscated by investigative organizations exceeded 1,000 kilograms, it can be assumed that smuggling of stimulants generates a large amount of criminal proceeds.

In addition, the reality is that criminal proceeds from drug-related crimes are important sources of revenue for Boryokudan, it can be illustrated by the fact that more than half of the persons arrested for illicit drug trafficking-related offenses in 2017 were Boryokudan gangsters. 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 process of stimulants (from shipping and receipt from overseas to central wholesale, intermediate wholesale, and distribution to end users in Japan).

Among overseas drug-related criminal organizations, Chinese, Mexican and West-African organizations have been increasing their presence, and criminal proceeds from drug-related crimes are an important source of revenue also for overseas criminal organizations. A breakdown of stimulant smuggling offenses by origin shows that China, Thailand, Taiwan, Malaysia,etc. occupy a large share. The breakdown of foreigners in Japan arrested for illicit stimulant trafficking by nationality shows that Iran occupies 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

As modus operandi of money-laundering offences related to illicit drug trafficking, there was a case in which payment was concealed and/or received by remittance to an account under the name of another person.

(2) Major Transactions etc. Misused for Money Laundering

We analyzed cleared cases of money laundering (3 years from 2015 to 2017) and counted the detected transactions etc. to be misused for money laundering while conducting criminal investigations.[*1]

There were 448 domestic exchange transactions[*2], 277 cash transactions and 110 deposit transactions that were misused fo 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 withdrawn from ATMs in cash in the end, making it very difficult to track the funds.

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

Table 6 [Major Transactions etc. Misused for Money Laundering (2015–2017)]

Misused transactions	Domestic exchange transactions	Cash transactions	Deposit transactions	International transactions (such as foreign exchange)	Legal person	Postal receiving service	Precious metals and stones	Electronic money	Credit card	Money lending	Insurance	Funds transfer services	Investment	Real estate	Safe-deposit box	Note/check	Legal/accounting professions	Virtual currency	Call forwarding service	Total
Total	448	277	110	45	21	15	14	10	5	5	5	4	4	4	3	3	3	2	1	979

Typical examples of misused transactions, etc. are:

○ Transferring criminal proceeds from fraud to accounts held in the name of another party (Domestic exchange transactions)

---

*1 This national risk assessment takes transactions etc. misused for concealing/receiving criminal proceeds, plus transactions etc. utilized for transforming criminal proceeds, as an object of analysis.

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

○ Converting stolen goods from theft offenses into cash by selling them in the name of another party (Cash transaction)
○ Depositing stolen cash in accounts in the name of another party (Deposit transaction)
○ Remitting criminal proceeds from fraud from a foreign country to an account in Japan (Transaction with a foreign country)
○ Remitting criminal proceeds from fraud to accounts of dummy corporation (Corporate status)[*1]
○ Receiving criminal proceeds from fraud through a postal receiving service (Postal receiving service)
○ Selling gold ingots acquired by fraud under the name of a legal person by using a friend of the offender (Precious Metals and Stones)

Cases of misusing those transactions etc. are individually explained in each item of "1. Major Products and Services in which Risk is Recognized" in "Section 3. Risk of Products and Services" in this report.

*1 Details of cases where legal person was misused for money laundering are explained in "Legal Persons without Transparency of Beneficial Ownership" in "Section 4. High Risk Transactions."

Section 3. 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 Institutions[*2]

A. Factor of Risks of Deposit-taking Institutions

(a) Characteristics

Deposit-taking institutions including banks are required to obtain licenses, etc. by the prime minister based on the Banking Act, etc. As of the end of March 2018, there are 1,394 institutions mainly consisting of banks (139 banks, excluding branches of foreign banks), cooperative financial institutions (Shinkin banks (261 banks), credit cooperative associations (148 associations), labor banks (13 banks), farmers' cooperatives and fisheries cooperatives (731 cooperatives) and federations of farmers' cooperatives and fisheries cooperatives (60 federations). Among these institutions, banks held a total deposit balance[*3] of 775,045.5 billion yen as of the end of September 2017.

Acceptance of deposits etc., loan of funds, discounting of bills, and exchange transactions (domestic and foreign exchange) are inherent business[*4] of deposit-taking institutions, while they also handle ancillary business such as consultation of asset management, sales of insurance products, credit card service, proposal for business succession, support for overseas expansion and business matching, etc.

In addition to banking operation mentioned above (including ancillary business), some banks which 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 (agent, examination, etc.), stock transfer agent business (management of stockholder list etc.), and inheritance-related business (execution of will, disposition of inheritance, etc.).

Deposit-taking institutions in Japan vary in the scale and scope of operation. Financial Services Agency, which is the competent authorities of deposit-taking institutions, classified them into major banks (mega banks) 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 expand internationally. Each regional bank and regional bank II have a certain geographic area where it mainly operates, but some regional banks have strategy to expand their business into several areas. 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. 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 risks of ML/TF in international society. As a matter of fact, cases have occurred recently in which some international crime organizations have passed funds illegally obtained by fraud, etc. in foreign countries through Japan's financial institutions in their process of money laundering.

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,

---

*1 This assessment report lists products and services according to the type of operator. However, each operator covers different scopes of product/service. Operators are required to consider the related contents in this report based on products/services they deal with.

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

*3 See "FY2017 interim Financial Statement Analysis of All Banks" by Japanese Bankers Association (116 banks are covered).

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

bills, and checks which are the products and services handled by deposit-taking institutions are as described below.

(b) STRs

There were 1,100,248 STRs by deposit-taking institutions from 2015 to 2017, accounting for 91.6% of total reports.

Among cases exampled in "List of Reference Cases of Suspicious Transactions,"[*1] major ones (and the number of reports) are as follows.

- ○ Unusual transactions or transactions related customers who show unusual behavior or movements, based on the knowledge and experience of staff (204,599 reports, 18.6%).
- ○ Transactions related to Boryokudan or its related parties (163,613 reports, 14.9%).
- ○ Transactions using accounts that frequently receive remittance from many persons. In particular, cases in which an account receives a remittance and a large amount of money is transferred or paid from the account immediately after such receipt of remittance (95, 971 cases: 8.7%)
- ○ Transactions that a huge amount of money is transferred from foreign countries without economic rationality (72,832 reports, 6.6%)
- ○ Transactions that deposits or withdrawals (including trade of securities, remittance, and currency exchange.: the same applies hereinafter) are involved. The same applies to the following.) are made in a huge amount of cash or a check, especially transactions with high value which are not proportionate to the customer's income or assets, or transactions that deposits or withdrawals dare to be made in cash although use of remittance or cashier's check seems to be reasonable (67,758 reports, 6.2%)
- ○ Transactions related to accounts through which a huge amount of money is frequently deposited or withdrawn (55,622 reports, 5.1%)
- ○ Transactions related to accounts which usually have no fund movement, but a huge amount of money is suddenly deposited to or withdrawn therefrom (55,284 reports, 5.0%)
- ○ Transactions that a huge amount of money is transferred to foreign countries without economic rationality (45,032 reports, 4.1%)
- ○ Deposits or withdrawals using accounts suspected to be opened by a fictitious or other person's name (37,799 reports, 3.4%)
- ○ 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 have been verified at the time of account opening (31,398 reports, 2.9%).
- ○ Transactions using accounts that frequently receive remittance from many persons. In particular, cases in which a large amount of remittance is received just before transfers are made (19,523 reports, 1.8%).

(c) Present Situation of Products/Services Dealt with by Deposit-taking Institutions and Misuse Case

(A) Deposit/Savings Account

a. Present Situation

Based on the reliabilities to deposit-taking institutions and fulfillment of a deposit protection system for a depositor, deposit/savings account is a popular and wide spread measure 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, deposit/savings account can be used as effective measures to receive and conceal criminal proceeds by those who attempt money laundering.

The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct verification at the time of transactions, and make and preserve verification records and transaction records when they conclude deposit/savings contracts (contracts about receipt of

*1 Competent administrative authorities provide "List of Reference Cases of Suspicious Transactions" to specified business operators. The list illustrates patterns which operators should especially pay attention to because they could fall under suspicious business transactions. When specified business operators file STRs, they are required to write a reference case which the transaction mainly fall into.

deposit/savings) with customers. The Act also requires deposit-taking institutions 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

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, such as suspension of transaction related to the account, when there is a suspicion about a deposit account to be misused for crimes, e.g. specialized fraud, based on information provided by investigative agencies or others regarding the deposit account.

b. Case

The following are example cases of misuse of deposit/savings accounts for money laundering:

- ○ Cases where accounts of foreign nationals who have returned to their home countries or deceased persons were used without the implementation of measures such as closure and in which criminal proceeds from fraud, theft, etc. were concealed.
- ○ Cases where offenders received or concealed criminal proceeds derived from fraud, theft, loan shark crime, drug crime, violation of amusement business act, etc., by the use of 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 acquisition of 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 of an underground loan being used for underground financial crimes, and members of Boryokudan using accounts under the name of a family member or friend in the case of gambling crimes, and accounts under the name of third parties or fictitious persons being used for specialized fraud crimes.

Furthermore, although the number of cases of misuse of accounts under corporate names is smaller than the number of cases of misuse of accounts 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 frauds 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 frauds, loan shark cases, etc. Proceeds are transferred through such accounts.

Police reinforce investigation on violation of the Act on Prevention of Transfer of Criminal Proceeds related to illegal transfer of deposit/savings passbook and cash card (see table 7). Looking at the number of arrests by nationality, Japan has the most followed by Viet Nam, China, and Korea. In particular, the number of cases of Japanese and Vietnamese arrests has been increasing recently.

In addition, the police also actively investigate cases of account fraud, in which offenders cheat deposit-taking institutions of deposit/savings passbook by falsely representing the location of a postal receiving service provider as their address at the time of account opening (account fraud), for example, while concealing the purpose of transferring it 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 violation of the Act on Prevention of Transfer of Criminal Proceeds (2015–2017)] Year

Category \ Year	2015	2016	2017
Transfer of deposit/savings passbook, etc. (business)	25	29	27
Transfer, etc. of deposit/savings passbook, etc. (business)	1,559	1,902	2,523
Solicitation for transfer of deposit/savings passbook, etc.	16	42	31
Transfer, etc. of exchange transaction cards, etc.	19	2	0
Others	0	4	0
Total	1,619	1,979	2,581

Note: Cleared cases in the "Others" category in 2016 are cases of false declaration of customer identification data to specified business operators.

Table 8 [Number of cleared cases of account fraud etc. (2015–2017)] Year

Category \ Year	2015	2016	2017
Account fraud	1,741	1,587	1,512
Transfer of stolen goods	12	4	6
Total	1,753	1,591	1,518

Note: Based on reports on crimes which promote specialized fraud, from prefectural police to the National Police Agency.

(B) Deposit Transactions

a. Present Situation

With the spread of ATMs through the 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 transaction") provide high convenience to account holders. People can prepare or preserve funds quickly and easily, regardless of time and place.

However, those who attempt money laundering could pay attention to safe and secure fund management of account and high convenience of deposit transactions and attempt money laundering through withdrawals of proceeds which were sent to the account or deposit of 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 conduct transactions of receipt or payment of cash which exceeds 2 million yen with customers (100,000 yen in the case of exchange transaction or including issuance of cashier's check). The Act also requires deposit-taking institutions 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

b. Case

The following are example cases of misuse of deposit transactions for money laundering:

- ○ A case where an offender withdrew criminal proceeds, which were derived from fraud in the foreign countries and transferred to an account in Japan, by disguising them as legitimate business proceeds
- ○ Cases where offenders concealed criminal proceeds derived from theft, fraud, embezzlement, drug crime, gambling, etc., by depositing them into accounts opened in another person's name
- ○ Cases in which an offender deposits a large amount of coins obtained by theft into another

person's account at an ATM operated by financial institutions and then the offender receives cash in bills

and so on.

(C) Domestic Exchange Transactions

a. Present Situation

Domestic exchange transactions are used for receiving remittance of salary, pension, dividend, etc. or paying utility fees, credit card charge, etc. by account transfer system. Domestic exchange transaction enables customers to make a safe and quick settlement without cash movement between remote areas. Because of such convenience, many people use it as a familiar settlement service with the spread of ATM and Internet banking.

On the other hand, domestic exchange transactions can be used as an efficient measure to commit money laundering because such 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 prepare and preserve verification records and transaction records when they conduct transactions of receipt or payment of cash that exceeds 100,000 yen in cash and include exchange transactions. The Act also requires deposit-taking institutions 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances. In addition, in the case of domestic exchange transactions involving the payment of funds to other financial institutions, when the receiving financial institutions request the paying financial institutions to conduct customer identification related to the transactions, the Act obligates the paying financial institutions to prepare records concerning matters that enable the search of the customers' records to be verified within three business days from the request date and obligates the receiving financial institutions to prepare records concerning matters that enable the search of information concerning the transactions.

b. Case

The following are example cases of misuse of domestic exchange transactions for money laundering

- ○ A case where a senior member of Boryokudan received criminal proceeds, which were derived from fraud by his acquaintance, by making him remit to the member's account
- ○ A case where an offender caused a third party to transfer a 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 offender took requests from more than one client and had them remit cash for an illegal overseas transfer of money into an account which the offender acquired for remuneration from a returned Vietnamese
- ○ A case where an offender sold obscene DVDs via cash-on-delivery postal service and made the delivery service provider remit the received money to an account opened in another person's name
- ○ Cases 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 person's name

and so on.

(D) Safe-deposit Box

a. Present 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, bankbook, bonds, deed or property, such as precious metals and stones.

However, as deposit-taking institutions do not check the stored items, goods in safe-deposit boxes have high secrecy. As a result, there are cases where criminal proceeds derived from violation of the Copyright Act and loan shark crimes were preserved in banks' safe-deposit boxes.

Because of such a characteristic, a safe-deposit box can be an effective measure 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 contracts of lease of safe-deposit boxes with customers. The Act also requires deposit-taking institutions 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

b. Case

The following are example cases of misuse of safe-deposit boxes for money laundering:

- ○ A case where an offender cheated a victim of his/her promissory note, converted it to cash, and preserved a portion of the cash in a safe-deposit box which was borrowed from a bank by his relative
- ○ There are cases 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 which was borrowed from a bank under the name of a family member

and so on. Also, in foreign countries,

- ○ There are cases where an offender concealed criminal proceeds by borrowing safe-deposit boxes with many banks by using false names

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

(E) Bills and Checks

a. Present Situation

Bills and checks are useful payment instruments which substitute for cash because they are used in clearance system with high credibility 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 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, bills and checks can be efficient means of receiving or concealing criminal proceeds because of such characteristics.

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 contracts of bill discount 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 not crossed (In the case where cash receipt and payment is involved and related to exchange transaction or checks drawn to self, 100,000 yen). The Act also requires deposit-taking institutions 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and

---

*1 Checks drawn as bearer checks stipulated in Article 5, paragraph 1, item 3 of the Check Act (Act No. 57 of 1933: "Act") 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.

other relevant circumstances.

Furthermore, 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 make verification at the time of transactions on opening accounts.

b. Case

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

○ Cases 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, and then checks were collected by deposit-taking institutions and transferred to accounts opened in the name of another party

and so on. Also, in foreign countries,

○ A case where bills or checks were misused to smuggle huge amount of funds

○ There are cases where bills or checks were misused by drug cartels as a means 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 means of transporting 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 administrative 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 carry out these obligations.[*2]

Furthermore, the Financial Services Agency has developed the "Guidelines regarding Measures for Money Laundering and Offer of Funds to Terrorism" in February 2018 and requires financial organizations to establish and maintain risk control systems for ML/TF.

(b) Measures by competent administrative authorities

The Financial Services Agency judges that deposit-taking institutions face relatively higher risks than other types of businesses taking into account the volume of financial transactions of 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 grasps the actual situation of compliance with laws and regulations and of risk control by documentary research and by report submission orders, executes risk assessment on types of business or business operators by gap analysis, etc. with said guideline and provides guidance or supervision, etc. corresponding to risks of business operators based on the results of the assessment.

As a result, it is made clear that although preparation of the specified business operator creation document 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 demands all business operators, regardless of their size, to implement risk assessment and it provides guidance and supervision to them with respect to their efforts toward the risk-based approach including the establishment and maintenance, etc. of the internal control system, by not simply focusing on formally checking the

---

*1 Regarding the Financial Services Agency's supervision over financial institutions, the Agency produces Comprehensive Guidelines for Supervision which 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 conduct proper AML/CFT measures at overseas business locations.

existence of violations of laws and regulations but also by placing importance on whether they have substantially responded based on the principle of the relevant laws and regulations, research documents or the Guideline.

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

(c) Measures by industry organizations and business operators

Regarding industry groups, they support AML/CFT measures of each business operator by providing case examples, supplying the database on subjects such as freezing assets, training, etc. In particular, the general incorporated association known as the Japanese Bankers Association develops organizational countermeasures in and outside Japan against ML/TF by following the checking situation of countermeasures for money laundering by FATF at any time, by continuously exchanging and sharing information with bankers associations in foreign countries and by responding to reciprocal examinations of Japan by FATF and it established the Government-Private Sector Coordination Meeting for Enhanced Countermeasures against Money Laundering in April 2018 to facilitate the coordination between the government and private sector and to further enhance countermeasures against money laundering. It also makes efforts to build a common recognition of countermeasures against money laundering between the government and private sector and in the industry as a whole through exchanging views and sharing of information at the Coordination Meeting.

Business operators themselves make efforts to establish and reinforce their AML/CFT internal control systems, too. For example, they set up a division in charge, develop internal regulations and manuals, 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 followings are recognized as examples of the risk assessment and of efforts for risk-based approach taken by business operators:

○ for those related to the identification of risks
- Cases where a company analyzes information on suspicious transactions reported by the company and extracts an independent risk index from the tendency of countries and regions of destination and origin regarding overseas transfers, tendency of nationality regarding accounts by names of foreigners and tendency of occupation or type of business regarding customers.
- Cases where a company, not only taking direct descriptions in assessment report into account, but also by taking into account the intent of the description, identifies specific risks where foreigners who are expected to be returning, such as students studying in Japan or short-term employees, may sell their accounts illicitly at the time of return or operators who mainly handle cash may receive a mixture of unauthorized funds in transactions.
- Cases where transactions using ordinary deposit accounts under foreigners' names in which movements including transfer of salary stopped or corporate accounts which were opened by applying with the teller for which the actual activities of the corporation could not grasped sufficiently by site inspection are specifically identified as high-risk transactions.

○ for those related to the risk assessment
- Cases where domestic exchange transactions are segmented into general transfers, salary transfers, tax payments, public utility charges, outward remittance, incoming remittance and so on and risks are assessed on each segment.
- Since transaction achievement of goods, customer types, geographical characteristics and so on vary by branch office, each branch office conducts its own analysis focusing on goods and services, transaction type, country/region, and attributes of customers.

○ for those related to the risk-based approach
- Cases where the case-by-case approval process is made clear in which, for example, a checklist for foreign remittance is prepared, and a teller of a branch office checks based on the list, and a general manager verifies and report to the responsible division of the headquarters.
- Cases where the duration of the visa of customers who are foreign workers or students is

checked and controlled by a system for the risk of sale of accounts at the time of their return;and

- Cases of banks that have a system of internal regulations in which accounts opened with a small amount, accounts of persons who live in a remote area, or accounts of corporations that have just been incorporated and relocated, and so on are designated as the control subject accounts and, if a request for 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 suspicious transaction is reported.

C. Assessment of Risks

Deposit-taking institutions provide various products and services, including accounts which secure safe fund management, deposit transactions which can make quick preparation or preservation of funds regardless of time and place, exchange transactions which can transfer funds between remote areas or many people in a quick and secure way, safe-deposit boxes which can provide safe preservation for property while maintaining secrecy, and bills and checks which are negotiable and easy to transfer.

On the other hand, these products and services can be convenient measures to transfer criminal proceeds because of characteristics they possess. Actually, there are cases where accounts, deposit transactions, exchange transactions, safe-deposit boxes, bills and checks were misused for receipt or concealment of criminal proceeds. Considering this situation, it is recognized that products and services of deposit-taking institutions have risks to be misused 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 in which cross-border crime syndicates 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.

In addition to statutory measures, competent administrative agencies and operators are taking the above-mentioned risk-mitigating measures against these risks, and the effects of such measures can be seen in the situation of effective efforts by operators.

However, the level of these efforts is different by operators, 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 and actual cases, it is recognized that transactions having the following aspects such as transaction conditions, customer types, etc. (excluding the transactions specified in "Section 4 High Risk Transactions"; the same applies to the following) would be exposed to higher risks.

- ○ Transactions that deposits and withdrawals are made in a huge amount of cash or checks (In the case of transactions which are made in large amounts and not proportionate to the customer's income or assets and transactions in which cash is deposited or withdrawn although it is considered to be appropriate to use remittance or cashier's check, it is recognized that risk will particularly increase)
- ○ Frequent transactions in a short period and deposits and withdrawals are made in a huge amount of cash or checks
- ○ Deposits, withdrawals, and safe-deposit box transactions in which it is suspected that names of account holders or safe-deposit box users are fictitious names, false names, or shell companies' names
- ○ Deposits and withdrawals through accounts of customers who hold many accounts (including

---

*1 Article 2, paragraph 2, item 35 of the Act on Prevention of Transfer of Criminal Proceeds provides that electronic monetary claim recording institution is specified business operator. Electronically recorded monetary claims are made or transferred when registry made of magnetic disk etc. and prepared by electronic monetary claim recording institutions is electronically recorded. Electronically recorded monetary claims have the function which is similar to bills regarding smooth assignment of obligation, so it is recognized that they have the risk to be misused for transfer of criminal proceeds.

*2 Article 2, paragraph 2, item 27 of the Act on Prevention of Transfer of Criminal Proceeds provides that a mutual loan company is specified business operator. In a mutual loan, a mutual loan company sets certain unit number and benefit amounts, clients regularly pay premiums, and they get property other than cash through lottery, bid, etc. every unit. Mutual loan has the characteristic which is similar to deposit regarding the system of premiums and benefits, so it is recognized that it has the risk to be misused for the transfer of criminal proceeds.

customers who hold many accounts under different names, including business names)

- ○ Transactions related to accounts that frequent or large amount deposits and withdrawals are made right after the account was opened, but it was cancelled or transactions stopped later
- ○ Transactions where cash is withdrawn from an account and the cash is transferred right after the withdrawal (including cases where the transaction is treated as cash transaction for slip process). (When remittance is made in a name different from the name of the holder of the account from which the withdrawal was made, it is recognized that risk will particularly increase)
- ○ Transactions related to accounts that frequent remittances are made to many people. (When a huge amount of money is deposited just before remittances, it is recognized that risk will particularly increase)
- ○ Transactions related to accounts that receive funds from many people frequently. (When large amounts of funds are transferred or withdrawn from the account right after the receipt of funds, it is recognized that risk will particularly increase)
- ○ Transactions related to accounts which receive remittance from persons suspected of using anonymity or fictitious names
- ○ Transactions related to accounts which usually have no fund movement, but a large amount of money is suddenly deposited to or withdrawn therefrom

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

A. Factors of Risks

(a) Characteristics

Basically, insurance contracts promise to pay insurance benefit in connection with the life or death of individuals or promise to compensate for damages caused by a certain incidental accident. Payment is limited to cases where those conditions, which have uncertainty, are met. This characteristic significantly mitigates the risks insurance has.

However, each insurance product varies on the characteristics. Insurance companies etc. provide some products which have cash accumulation features. Unlike insurance products that provide benefit based on incidental accidents, some products with cash accumulation features provide benefit based on conditions which are more certain to be met, such as maturity. These products may, in many cases, provide a considerable amount of cash surrender value when contracts are cancelled before maturity.

As of the end of 2018, there were 96 companies which had obtained a license from the prime minister based on the Insurance Business Act (Act No. 105 of 1995).

(b) STRs

There were 7,610 STRs by insurance companies, etc. from 2015 to 2017 (6,840 in life insurance and 746 in general insurance and 24 in mutual- aid program). Among cases exampled in "List of Reference Cases of Suspicious Transactions," major one (and the number of reports) in the life insurance sector is as follows.

○ Transactions related to Boryokudan or its related parties (5,484 reports, 80.2%)

and in general insurance,

○ Transactions related to Boryokudan or its related parties (534 reports, 71.6%)

○ Unnatural transactions or transactions related to customers who show unnatural behavior or movements based on the knowledge and experience of staff (164 reports, 22.0%)

cases.

Furthermore, in the life insurance sector, there are a certain number of STRs focusing on payment of premium in a lot of cash (48 reports, 0.7%), including an STR where a customer made payment in a lump sum in cash, 15 million yen, for premium.

(c) Case

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

○ A case where a drug trafficking organization spent their drug proceeds on the purchase of life insurance, then soon cancelled the insurance and received refund

and so on. The following are example cases where criminal proceeds were transformed in Japan:

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

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 contract of insurance with cash accumulation features, when

---

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

a contractor of such insurance is changed, when they make payment of maturity insurance money, cash surrender value, etc. of such insurance, and when they make transactions for receiving and paying cash more than 2 million yen. The Act also requires insurance companies 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result ofverification at the time of transactions the actual manner of the transactions and other relevant circumstances.

Moreover, in addition to the supervisory measures based on the Act, the Insurance Business Act provides that competent administrative authorities can require submission of reports from, issue business improvement orders to or conduct on-site inspection of insurance companies if necessary. In Comprehensive Guidelines for Supervision of Insurance Companies, focal points include the development of internal control systems regarding conducting verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds.

(b) Measures by competent administrative authorities

The Agency demands operators to establish and maintain the risk control system against ML/TF based on the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" and grasps the actual situation of compliance with laws and regulations and of risk control by documentary research and by report submission orders, executes risk assessment on types of business or operators by gap analysis, etc. with said guidelines and provides guidance or supervision, etc. corresponding to risks of operators based on the results of the assessment.

(c) Measures by industry organizations and business operators

In order to prevent insurance from being misused for wrongful fundraising, Life Insurance Association of Japan and General Insurance Association of Japan introduced a system which enables member companies to register contents of their contracts and to refer to them when necessary. This system facilitates information sharing among member companies. When they receive application for contract or for payment of insurance benefit, they can refer to the system to examine whether any suspicious situations exist (for example, an insured person has several insurance contracts which are the same type). The Associations also create various materials, such as handbooks and Q&A, to support AML/CFT measures taken by member companies.

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 audit, screen out transactions that are considered at high risk, and adopt enhanced monitoring for transactions at high risk.

C. Assessment of Risks

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

Actually, there are cases where money laundering related to violation of the Anti-Prostitution Acts were used to buy insurance products with cash accumulation features. Considering a relevant situation, it is recognized that such insurance products have risks that can be exploited for ML/TF.

Competent administrative agencies and operators are taking, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts is different by operators, 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.

Furthermore, based on STRs, actual cases, etc., it is recognized that transactions having the following aspects such as transaction conditions, customer types, etc. would be exposed to higher risks.

○ Transactions related to contractors who pay premiums in a lot of cash

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

A. Factors of Risks

(a) Characteristics

Besides deposit at deposit-taking institutions, investment in stocks, bonds, and other investment products is also a useful way to manage funds. Investment instruments include commodity derivatives transactions of minerals and agricultural products, as well as financial products, such as stocks, bonds, and investment trusts.

As of the end of March 2018, there were 4,192 companies which had been registered by or notified to the prime minister based on the Financial Instruments and Exchange Act (Act No. 25 of 1948) and 45 companies which 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).

Surveying investment transactions in Japan, total transaction volume of stocks listed on the Tokyo Stock Exchange, Inc. (First Section and Second Section) is about 695.9627 trillion yen in 2017 (see table 9).

Regarding commodity derivatives transactions, trading volume at commodity exchanges in Japan (Tokyo Commodity Exchange, Inc. and Osaka Dojima Commodity Exchange) is about 24.53 million contracts[*2] in 2017. Total value is about 51.7754 trillion yen in 2017, and clearing margin balance at the end of December is about 177.3 billion yen (see table 10).

Investment has different characteristics from deposit/savings. Customers take risks of losing principal when value of investment targets fluctuates. However, at the same time, they can obtain more profit than deposit/savings if the investment succeeds.

From the viewpoint of risks to be misused for ML/TF, investment can be used to convert a lot of funds into various products. In addition to that, some investment instruments consist of complicated schemes and can be used to make source of funds unclear and tracking of money laundering difficult.

Table 9 [Transaction Volume of Stocks (2015–2017)]

(Unit : million yen)

Category \ Year	2015	2016	2017
First Section, TSE	696,509,496	643,205,780	683,218,254
Second Section, TSE	8,266,622	6,118,918	12,744,471
Total	704,776,118	649,324,718	695,962,725

Note: Data from Tokyo Stock Exchange

Table 10 [Transaction Amount of Commodity Derivatives Transactions (Domestic Commodity Exchanges) (2015–2017)]

Category \ Year		2015	2016	2017
Volume (number of contracts) (Sheet)	Agricultural products	1,063,389	975,802	665,435
	Minerals	23,748,554	26,402,832	23,866,328
Transaction amount (100 million yen)		622,336	588,617	517,754
Margin balance (end of December) (100 million yen)		1,332	1,516	1,773

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.

---

*1 Here, financial instruments business operators, etc.commodity derivatives business operators,refer to operators listed in Article 2, paragraph 2, item 21 (financial instruments business operator), item 22 (securities finance company), item 23 (specially permitted business notifying person), and item 32 (commodity derivatives business operator) of the Act on Prevention of Transfer of Criminal Proceeds.

*2 "Sheet" is the name of the minimum transaction unit showing transaction volume or delivery volume which constitutes the base for transaction in the exchange.

(b) STRs

There were 25,915 STRs by financial instruments business operators, etc. and 42 STRs by commodity derivatives business operators from 2015 to 2017. Among cases exampled in "List of Reference Cases of Suspicious Transactions," major one (and the number of reports) by financial instruments business operators, etc. is as follows.

○ Tradings of stocks, securities, and investments in investment trusts, etc., using accounts suspected to be opened by a fictitious or other person's name (8,142 reports, 31.4%)

and, in the case of the commodity derivative business operators

○ Transactions suspected that the customer uses a fictitious or other person's name (14 reports, 33.3%)

cases.

(c) Case

The following are example cases of misuse of investment for money laundering through financial instruments business operators, etc. and commodity derivatives business operators:

○ A case where an offender remitted criminal proceeds derived from fraud into an account in a securities company which was opened by a false name and the offender purchased stocks

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

○ A case where criminal proceeds derived from embezzlement in the pursuit of social activities 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

Furthermore, in addition to the supervisory measures under the Act, the Financial Instruments and Exchange Act and the Commodity Derivatives Act provide that competent administrative 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 to Financial Instruments Business Operators, etc. and commodity derivatives business operators include focal points on the development of an internal control system regarding conducting verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds.

(b) Measures by competent administrative authorities

The Financial Services Agency demands financial instruments business operators, etc. who are under its jurisdiction to establish and maintain the risk control system against ML/TF based on the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" and grasps the actual situation of compliance with laws and regulations and of risk control by documentary research and by report submission orders, executes risk assessment on types of business or operators by gap analysis, etc. with said guideline and provides guidance or supervision, etc. corresponding to risks of operators based on the results of the assessment. Furthermore, as a part of its year-round monitoring activities for financial instruments business operators, etc. the Financial Services Agency verifies the current situation of measures taken for ML/TF.

Furthermore, the Ministry of Agriculture, Forestry and Fisheries and the Ministry of Economy, Trade and Industry also perform documentary research to grasp the actual situation of compliance with laws and regulations and risk control by commodity derivatives business operators who are

under its jurisdiction and it provides guidance and supervision corresponding to the risks of respective commodity derivatives business operators based on information obtained by the research and orders. The Ministry of Land, Infrastructure, Transport and Tourism, etc also performs documentary research and issues report submission orders to grasp the actual situation of compliance with laws and 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 by the research and orders.

(c) Measures by industry organizations and business operators

Japan Securities Dealers Association[*1] and The Commodity Derivatives Association of Japan[*2] create Q&As or other materials regarding the Act on Prevention of Transfer of Criminal Proceeds, etc. to support AML/CFT measures taken by member companies. Japan Securities Dealers Association also creates "Point of view about 'STRs' for members" to help members have deeper understanding about STRs and to ensure STRs are properly made. Furthermore, the Association shows specific examples and matters to be noted which are useful for member companies when dealing with actual business relating to the "Guideline for Anti Money Laundering and Combating the Financing of Terrorism" prepared by the Financial Services Agency and promotes appropriate response to ML/TF.

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

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 customers are allowed to transfer funds only to accounts with his/her own name, but not to third parties in principle. This may be a measure to mitigate the degree of risks of investment if remittance and payment by different names is appropriately controlled.

C. Assessment of Risks

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

In addition, some of these investment products have complex scheme which can make tracking source of invested funds difficult. Therefore, investment 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 in the pursuit of social activities were invested in stocks or commodity derivatives. Considering a relevant situation, it is recognized that investment made through financial instruments business operators, etc. and commodity derivatives business operators may involve risks to be misused for ML/TF.[*3] [*4]

---

*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 for sound development of the industry and protection of investors, including by setting up self-regulatory rules. As of the end of March 2018, 264 Type I financial instrument business operators join the Association as members and they have the obligation to comply with the rules of the Association.

*2 The Commodity Futures Association of Japan is a self-regulation organization which is approved under the Commodity Derivatives Act. The Association conducts various self-regulation works regarding commodity derivatives business for fair and smooth commodity derivative transactions and protection of clients. All commodity derivatives business operators join the Association and they have the obligation to comply with the rules of the Association.

*3 Article 2, paragraph 2, item 26 of the Act on Prevention of Transfer of Criminal Proceeds provides that a specified joint real estate enterprise is a specified business operator. 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 excute 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 measure to make tracking criminal proceeds difficult, therefore, has risks to be misused for ML/TF.

*4 Article 2, paragraph 2, items 33 and 34 of the Act on Prevention of Transfer of Criminal Proceeds provide that a Book-entry transfer institution and an account management institution are specified business operators. Book-entry transfer institutions

Competent administrative agencies and operators are taking, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts is different by operators, 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 having the following aspects such as transaction conditions, customer types, etc. would be exposed to higher risks.

○ Transactions suspected that the customer uses a fictitious or other person's name

conduct the business of book-entry transfer (which has the effect of transfer, pledge, etc.) of company bonds etc. Account management institutions, which securities companies, banks, etc. are allowed to be, open the account for the purpose of effecting the book-entry transfer of company bonds etc. on behalf of another person. Products and services handled by these institutions have risks to be misused for ML/TF.

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

A. Factors of Risks

(a) Characteristics

Trust is a system where a settlor transfers cash, land, or other property to a trustee by act of trust and the trustee manages and disposes the property for a beneficiary pursuant to the trust purpose set by the settler. In trust, assets can be managed and disposed in various forms.

Trustees make the best use of their expertise to manage and preserve assets. Trust is an effective way to raise funds for companies. With these characteristics, trust is widely used in schemes for managing financial assets, movable property, real estate, etc. as a basic infrastructure of financial system in Japan.

In order for a person to operate a trust business as a trust company, the person is required to obtain the registration, license or authorization by competent administrative authorities based on the Trust Business Act (Act No. 154 of 2004), and when banks and other financial institutions operate trust business, they are required to obtain approval by competent administrative authorities under the Act on Engagement in Trust Business by a Financial Institution (Act No. 43 of 1943). As of the end of March 2018, 64 companies were engaging in trust business with such a license and authorization.

No money laundering case involving misuse of trust has been reported in Japan in recent years. However, trust is not only to leave property with trustees but also has the function of changing the nominee of property right and transferring a right of management and disposal 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, trust can be effective means of concealment of the source of illegal proceeds.

(b) STRs

There were 37 STRs[*2] related to trusts from 2015 to 2017. Among cases exampled in "List of Reference Cases of Suspicious Transactions," major ones (and the number of reports) are as follows.

○ Transactions related to Boryokudan or its related parties (23 reports, 62.2%)

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 conducting conclusion of a contract for trust or a conclusion of judicial relationship with a beneficiary of trust through acts, including act of trust, act of designation of a beneficiary, act of transferring a right to be a beneficiary, excluding 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 the case where management systems for verification at the time of transactions have 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 indicates focal points for trust companies and financial institutions that operate trust business with respect to the development of internal control systems regarding verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds. Specified business operators themselves also make efforts to establish and strengthen their AML/CFT internal control

---

*1 Trust Companies etc. mean operators 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, information of STRs was analyzed and relations with trusts was confirmed.

systems. For example, they set up a division in charge, develop internal regulations and manuals, provide periodic training, conduct internal audit, screen out transactions that are considered at high risk, and adopt enhanced monitoring for transactions at high risk.

Moreover, trustees are required to submit records including beneficiaries' names to tax authorities under the tax law, excluding some trusts. This system is not directly for AML/CFT purpose, but helps competent administrative authorities to identify beneficiaries of trusts.

In addition, funds related to trust, such as proceeds from trust assets and payment for a trust beneficiary right are transferred through bank accounts. Therefore, it can be said that measures to mitigate risks such transactions have are doubly taken by laws and regulations related to AML/CFT regime against the deposit-taking institution sector, supervision by competent administrative authorities, and voluntary efforts by industry and business operators.

(b) Measures by competent administrative authorities

The Agency demands operators to establish and maintain the risk control system against ML/TF based on the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" and grasps the actual situation of compliance with laws and regulations and of risk control by documentary research and by report submission, executes risk assessment on types of business or operators by gap analysis, etc. with said guidelines and provides guidance or supervision, etc. corresponding to risks of operators based on the result of such assessment.

C. Assessment of Risks

Trust has the function of transferring property right from a settlor to a trustee, changing the nominee of the property when it is subject to a registration system, and altering attribution, quantity and nature of the property. Furthermore, trust can come into force on conclusion of a trust contract between parties involved or self-settled trust. Because of such characteristics, for those who attempt ML/TF, it is possible to separate criminal proceeds from themselves and conceal the relationship with the proceeds if they misuse trust. No money laundering case arrest involving misusing trust has been reported in Japan in recent years. However, by these characteristics, trust can be considered to be risky in misusing for ML/TF.

Competent administrative agencies are taking, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts is different by operators, 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.

(5) Money Lending Dealt with by Money Lenders etc.*1

A. Factors of Risks

(a) Characteristics

Lending money or acting as an intermediary for lending money (hereinafter referred to as "money lending", collectively) by money lenders etc. helps consumers and business operators, who need funds, raise money, by providing them with convenient financing products and carrying out quick examination, 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 service has become more convenient.

By making use of such convenience of money lending, those who obtained criminal proceeds can make tracking criminal proceeds difficult by misusing money lending, for example, by repeating debt and repayment.

In order to engage in money lending business, it is necessary to be registered by a prefectural governor or the prime minister (when a company seeks to do business with sales branches and business offices in two or more prefectures). As of the end of March 2018, there were 1,770 registered companies, while the outstanding balance of loans was 23,508.4 billion yen as of the end of March 2018.

(b) STRs

There were 17,202 STRs by money lenders etc. from 2015 to 2017. Among cases exampled in "List of Reference Cases of Suspicious Transactions", major ones (and the number of reports) are as follows.

- ○ Transactions related to Boryokudan or its related parties (7,212 reports, 41.9%)
- ○ Deposits or withdrawals using accounts suspected to be opened by a fictitious or other person's name (6,053 reports, 35.2%)

(c) Case

The following are examples cases where proceeds derived from crimes were transformed:

- ○ Cases where proceeds derived from armed robbery and fraud were spent on repayment for money lenders

and so on.

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, and to prepare and preserve verification records and transaction records on money lenders etc. when they make contract of money lending. The Act also requires money lenders 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

In addition to the supervisory measures based on the Act, the Money Lending Business Act stipulates that the competent administrative authorities can conduct on-site inspection of, require submission of reports from or issue business improvement orders to money lenders etc. Comprehensive Guidelines for Supervision of Money Lenders include focal points on the development of internal control systems regarding conducting verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds.

---

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

(b) Measures by competent administrative authorities

The Agency demands operators to establish and maintain the control system against ML/TF based on the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" and grasps the actual situation of compliance with laws and regulations and of risk control by documentary research and by report submission, executes risk assessment on types of business or operators by gap analysis, etc. with said guidelines and provides guidance or supervision, etc. corresponding to risks of operators based on the result of such assessment.

(c) Measures by industry organizations and business operators

Japan Financial Services Association has made self-regulating rules which 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 and STRs and prevention of damage caused by anti-social forces.

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. has risks to be misused for ML/TF.

Competent administrative agencies and operators are taking, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

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

In addition, based on STRs, actual cases, etc., it is recognized that transactions having the following aspectss such as transaction conditions, customer types, etc. would be exposed to higher risks.

○ Money lending contracts suspected that the customer uses a fictitious or other person's name

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

A. Factors of Risks

(a) Characteristics

Funds transfer service means exchange transaction services (limited to transactions that 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 service along with the spread of the internet etc., funds transfer service was introduced in 2010, to promote deregulation.

Those who intend to operate funds transfer service are required to be registered by the Prime Minister under the Payment Services Act. As of the end of March 2018, there were 58 registered companies. There were 84 million remittances totaling 1,087.7 billion yen in fiscal 2017. With the advance of globalization, it is expected that needs for funds transfer service, such as remittance by foreign people in Japan to their home countries, will increase further (see table 11).

There are three main remittance methods in funds transfer service. One is that a client requests fund transfer by bringing cash to a sales office of a Funds Transfer Service Provider and a receiver receives cash at the provider's different business location. Another is that fund is transferred between a client's account and a receiver's account which were opened in a funds transfer service provider. The other is that a Funds Transfer Service Provider issues a card or an instrument (money order) correspondent to money recorded in its server and payment is done to a card holder or a person who brings the instrument.

Funds transfer service is a convenient system providing a quick and secure way to transfer funds on a global scale with reasonable fees. However, the service facilitates transferring criminal proceeds to foreign countries where law or transaction systems are different from Japan and decreases traceability of the criminal proceeds.

Table 11 [Number of Performance by Funds Transfer Service (2015–2017)]

Year / Category	2015	2016	2017
Number of remittances a year	25,937,434	41,609,029	84,071,614
Transaction volume a year (million yen)	547,978	748,156	1,087,737
Number of registered funds transfer service providers	44	48	58

Note: Data from the Financial Services Agency

(b) STRs

There were 2,406 STRs by fund transfer service providers from 2015 to 2017. Among cases exampled in "List of Reference Cases of Suspicious Transactions," major ones (and the number of reports) are as follows.

- ○ Transactions having unnatural aspects or conducted in unnatural frequency considering the purpose of the transactions, occupation or business of the client, etc. (236 reports, 9.8%)
- ○ Deposits or withdrawals using accounts suspected to be opened by a fictitious or other person's name (141 reports, 5.9%)
- ○ Frequent transactions in a short period and deposits and withdrawals are made in a huge amount of cash or checks (the same rule applies to cases where transactions whose value is slightly below the threshold value is recognized) (106 reports, 4.4%)
- ○ Transactions on accounts which transfer remittance funds to lots of persons frequently. In particular, cases in which a large amount of remittance is received just before transfers are made (99 report, 4.1%)
- ○ Transactions that deposits or withdrawals (including trade of securities, remittance, and currency exchange.: the same applies hereinafter) are involved. In particular, transactions that deposits or withdrawals (including trade of securities, remittance, and currency exchange) are made in a huge amount of cash or a check, especially transactions with high value which are not proportionate to the customer's income or assets, or transactions that deposits or

withdrawals dare to be made in cash although use of remittance or cashier's check seems to be reasonable (72 reports, 3.0%)

On top of that, funds transfer service providers made some STRs about Money Mule [*1] in recent years. In the STRs, typically, a fund transfer service provider asked a customer the purpose of remittance and found out that he had applied to a job offer on a foreign website and had received money and instruction to forward the money to a foreign country.

(c) Case

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

- ○ Cases including a case of Money Mule where a person was asked to remit money overseas with reward and carried out the remittance through a funds transfer service provider while knowing that the remittance had no justifiable reasons
- ○ A case where a Dangerous Drugs (New Psychoactive Substances) trafficker concealed his proceeds into an account opened in other person's name, then remit the money overseas through a funds transfer service provider in order to buy material to produce the Drug
- ○ A case where a person, who operated unlicensed international remittance business, restocked funds which had to be pooled in the remittee country through a funds transfer service provider
- ○ Cases where an offender transfers criminal proceeds derived from the sale of a grifted car to foreign countries using fund transfer service provider

and so on. In the past, there were cases in which an offender transferred criminal proceeds derived from illicit transfer case 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 Funds Transfer Service Providers to conduct verification at the time of transactions, and prepare and preserve verification records and transaction records when they make exchange transactions etc. which accompany receiving and paying cash more than 100,000 yen. The Act also requires transfer service providers 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

Moreover, in addition to the supervisory measures based on the Act, the Payment Services Act provides that the competent administrative 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 which include "a corporation who has not established a system that is necessary for the proper and secure provision/conducting of funds transfer service". The Guidelines for Administrative Processes by the Financial Services Agency include focal points on the development of internal control system regarding conducting verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds. When business operators apply for registration of 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 service". Through these measures, competent administrative authorities provide AML/CFT guidance and supervision.

(b) Measures by competent administrative authorities

---

*1 A method of money laundering. In Money Mule, a third party is utilized as a carrier of criminal proceeds. Third parties are recruited through email or recruitment websites, etc.

The Agency demands operators to establish and maintain the risk control system against ML/TF based on the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" and grasps the actual situation of compliance with laws and regulations and of risk control by documentary research and by report submission order, executes risk assessment on types of business or operators by gap analysis, etc. with said guidelines and provides guidance or supervision, etc. corresponding to risks of operators based on the result of such assessment.

Furthermore, the Agency strengthens its efforts on supervision placing emphasis on transfer transactions in particular by executing research on transfer transactions.

(c) Measures by industry organizations and business operators

In the industry, Japan Payment Service Association supports AML/CFT measures taken by Funds Transfer Service Providers through developing self-regulating rules, providing training, etc.

Besides, Funds Transfer Service Providers 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 audit, screen out transactions that are considered at high risk, and adopt enhanced monitoring for transactions at high risk.

Business schemes of Funds Transfer Service Providers vary. Some of them, for example, who can conduct international remittance to many countries or accept occasional customers have risks to be misused for ML/TF. On the other hand, some providers, for example, who deal with only refund for cancelled mail order have 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 midsized enterprises, but if the nature of business to be handled is same, peculiar risks of being misused for ML/TF are not basically different considerably. However, it is acknowledged that, although the establishment of the internal control system of fund transfer services providers is sufficient in the case of large-scale operators at present, but since such establishment is insufficient in the case of small and medium sized enterprises, the Financial Services Agency tries to level-up the countermeasures against ML/TF of the industry as a whole by providing appropriate guidance and supervision including administrative guidance to operators whose efforts are insufficient.

C. Assessment of Risks

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

Actually, there are cases where criminal proceeds were transferred overseas through funds transfer service, by using a third party who was not involved in predicate offenses or by using another person's ID to pretend to be the person. Considering a relevant situation, it is recognized that funds transfer service has risks to be misused for ML/TF.

Furthermore, since the deposit-taking financial institutions are strengthening their AML/CFT countermeasures, there are concerns in which persons attempting to conduct ML/TF use fund transfer services operated by fund transfer services providers in lieu of goods and services handled by the deposit-taking financial institutions. These circumstances increase the degree of risks of fund transfer services.

Against such degree of risks, competent administrative agencies and operators take, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts is different by operators, 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 having the following aspects such as transaction conditions, customer types, etc. would be exposed to higher risks.

○ Remittances originated from cash etc. which are conducted frequently in a short period and large in total (including a case where some of the remittances are slightly below the threshold)

- ○ Transactions suspected that the customer uses a fictitious or other person's name
- ○ Transactions having unnatural aspects or conducted in unnatural frequency considering the purpose of the transactions, occupation or business of the client, etc.
- ○ Transactions suspected that the customer acts on behalf of other people

(7) Virtual Currency Dealt with by Virtual Currency Exchange Service Providers

A. Factors of Risks

(a) Characteristics

In Japan, virtual currency 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) which can be used to pay unspecified persons, when purchasing goods, etc., for the repayment of the price and which can be purchased from and sold to unspecified persons as the counter party and is a currency which can be transferred using electronic information processing systems.

The transaction amount of these virtual currency is increasing globally including Japan, and, as a result, the occurrence of cases involving virtual currency is recognized. In Japan, 149 cases of unauthorized transmission by unauthorized access to Virtual Currency Exchange Service Providers with damages of about 662.4 million yen occurred in 2017. And, in January and September 2018, cases where a huge amount of virtual currency seemed to be illicitly transmitted from domestic virtual currency exchange service providers occurred.

In the background behind some of these cases are circumstances in which the establishment of appropriate internal control systems for risks of various kinds including money laundering could not keep up with the rapid expansion of the business scale of operators handling virtual currency.

Most virtual currency like Bitcoin have characteristics in which their transaction history is published on the blockchain so their transactions can be traced. However, if wallets used for transactions are acquired or controlled by virtual currency exchange service providers or individuals in countries or regions where measures for identification of the principal, etc., is not mandatory, it becomes difficult to identify the owner of the virtual currency transferred in a transaction.

And, since almost all transactions of virtual currency exchange service providers are not conducted in person but over the internet, they have high anonymity, relatively speaking. In addition, some virtual currency are made more anonymous with anonymization technologies to make the connection between transfer origin and transfer destination vaguer. If virtual currency that have been made even more anonymous are exchanged in transactions, subsequent tracking of those transactions is that much more difficult.

With respect to the exchange of virtual currency and legal currency, virtual currency ATMs by which virtual currency and legal currency can be exchanged are located in some foreign countries, which make it possible to get virtual currency cashed or to purchase virtual currency by cash and improve the convenience for users. It is expected that virtual currency exchange service providers may study the possibility of establishing virtual currency ATMs or increasing the number of units in anticipation of the increase in demand. However, since cases are occurring in foreign countries in which drug traffickers exchange proceeds derived from drug trafficking into virtual currency by virtual currency ATMs, it is necessary to watch how such ATMs are actually being used.

In order to engage in the virtual currency service business, it is necessary to be registered by the prime minister based on the Payment Services Act. As of October 1, 2018, there are 16 companies (or 19 if deemed virtual currency exchange service operators are included).

FATF prepared the "Guidance on Virtual Currency" in June 2015 and pointed out that users of virtual currency were of high anonymity and that the transfer of virtual currency was conducted globally and promptly, and FATF is now updating the Guidance. FATF also revised its "40 New Recommendations"(Recommendation 15) in October 2018 and demands each country to impose regulations for countermeasures against ML/TF, on service providers who exchange virtual currency with legal currency and to introduce the license system or registration system for such providers.

(b) STRs

The number of STRs from virtual currency exchange service providers during the period from April to December 2017 was 669 reports. Many reports, including some that focused on customer information, identified many suspicious transactions using fictitious names or other people's names, the content of which includes,

○ 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 is made from the same IP address
○ The country of residence of a user is Japan, but the service is being logged into from outside Japan
○ The same mobile phone number is registered as the contact for more than one account or user, but the phone number is not in use

and so on.

(c) Case

The following are example cases of misusing virtual currency for money laundering:

○ Cases where an offender purchased virtual currency using illicitly acquired accounts or credit card information under other person's name, exchanged into Japanese yen using exchange sites in foreign countries and transferred the proceeds to accounts under another person's name

have been found.

And, as cases of violation of the Act on Prevention of Transfer of Criminal Proceeds in which an offender impersonates another person and accepts the required ID and passwords for the purpose of receiving services under a contract for virtual currency exchange with a virtual currency exchange service providers.

○ Cases where an offender offered IDs and passwords for virtual currency accounts opened by foreigners in Japan to third parties for a price
○ Cases where an offender opened accounts with virtual currency exchange service providers using the principal identification documents of another person

have been found.

Other cases where virtual currency was used as the means of payment in crimes:

○ Cases where virtual currency was used for transactions of illegal drugs or for payment of special points which 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 virtual currency exchange service providers to conduct verification at the time of transactions and to prepare and preserve the verification records and transaction records when concluding contracts concerning continuous or repeated exchange of virtual currency (conclusion of contracts concerning opening of wallets), when converting virtual currency worth more than 2 million yen and when transferring virtual currency of customers, etc., worth more than 100,000 yen upon the customers' request. The Act also requires Virtual Currency Exchange Service Providers 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances. 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 virtual currency exchange with a virtual currency exchange service provider.

In addition to supervisory measures based on the Act, if a person operates a virtual currency service, the person is required to be registered by the prime minister and assumes the obligation of submitting reports under the Act on Settlement of Funds. The Act stipulates that the competent administrative authorities may enter their offices for inspection and issue business improvement orders, etc., to virtual currency service operators if necessary. In addition, the Act also provides the grounds for refusing or rescinding the registration of a virtual currency exchange service providers, which include "a corporation who has not established a system that is necessary for the proper and secure conducting of virtual currency exchange service business." Moreover, the Guidelines for Administrative Processes by the Financial Services Agency include focal points

related to the development of internal control systems regarding verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds. When business operators apply for registration as a virtual currency exchange service provider, these points are also included in the examination items related to "establishing a system that is necessary for the proper and secure conducting of virtual currency exchange service business." Through these measures, the system for the guidance for AML/CFT by the competent administrative authorities is introduced, and the administrative guidance is actually executed.

(b) Measures by competent administrative authorities

For the purpose of strengthening guidance and supervision on virtual currency exchange service providers, the Financial Services Agency developed the "Guidelines for Administrative Processes" in April 2017 for employees in the Agency for the supervision on virtual currency exchange service providers and, in August of said year, facing increasing risks of ML/TF, involving virtual currency, established the Virtual Currency Monitoring Team to strengthen guidance and supervision on virtual currency exchange service providers and to perform the examination which places importance on the substantial effectiveness of the internal systems of virtual currency exchange service providers. Based on the Guidelines, the Financial Services Agency issues warnings to corporations operating virtual currency exchange service and issued two warnings as of October 1, 2018.

In addition, the Agency requires virtual currency exchange service providers to establish and maintain a control system against ML/TF, based on the "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism" and grasps the actual situation of compliance with laws and regulations and of risk control by report submission and provides guidance or supervision, etc., corresponding to risks of operators based on the results of the assessment.

The Financial Services Agency executed administrative action of business suspension orders or business improvement orders to virtual currency exchange service providers, etc., falling under the following cases:

- ○ Cases where the verification at the time of transactions and the judgment on the necessity of STRs are not performed in connection with the sale and purchase of a large amount of virtual currency more than one time
- ○ Cases where virtual currency exchange services are offered without sufficiently performing the verification at the time of transactions
- ○ Cases where the system to confirm the verification at the time of transactions is not in place and training for the verification is not performed for employees
- ○ Cases where, although the Agency had given guidance, no corrections were made since no person is available who sufficiently understands the content of the request for correction

For the reasons mentioned above, the Agency executed administrative actions of 28 business suspension orders and business improvement orders as of October 1, 2018.

(c) Measures by industry organizations and business operators

As their own efforts, 16 virtual currency exchange service providers established the General Incorporated Association Japan Virtual Currency Exchange Services in March 2018, which is a new industry organization, and developed self regulation rules based on the "Guidance on Anti-Money Laundering and Terrorist Financing Measures" of the Financial Services Agency. The Association was designated as an authorized funds settlement operators association based on the Act on Settlement of Funds by the Financial Services Agency in October of the same year.

C. Assessment of Risks

Major characteristics of virtual currency is that its users are highly anonymous and that the transfer of virtual currency can be quickly conducted across national borders. In addition, the regulation of virtual currency differs from country to country. In light of these factors, if virtual currency is misused for crimes, it becomes difficult to trace the proceeds derived from the crimes.

In consideration of actual cases where the anonymity of virtual currency was misused to convert illegally obtained virtual currency into cash through a virtual currency exchange service provider and have the money remitted to an account opened in another person's name, it is recognized that virtual currency is at risk of being misused for ML/TF.

And, considering that virtual currency transactions are increasing globally and the environment surrounding such transactions is rapidly changing, it is recognized that the level of risk in which virtual currency is misused for ML/TF, is relatively high in comparison to other types of business. Furthermore, since the deposit-taking financial institutions are strengthening their AML/CTF countermeasures, there are concerns that persons attempting to conduct ML/TF will use virtual currency transactions in lieu of goods and services handled by the deposit-taking financial institutions. These circumstances increase the degree of risks of virtual currency.

Against such degree of risks, competent administrative agencies and industry organizations execute risk-mitigating measures as mentioned above in addition to statutory measures, and, by these measures, the effect of risk-mitigating measures are shown to a certain extent as seen in the facts that the number of reports of suspicious transactions by operators substantially increases or that operators who fail to take appropriate money laundering measures receive a business suspension order and is caused to suspend its services.

However, it is not easy to take appropriate risk-mitigating measures in a timely manner amid rapid changes in environment surrounding virtual currency transactions, and if such efforts are insufficient, appropriate mitigating measures cannot be taken and the degree of risks is still high.

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

A. Factors of Risks

(a) Characteristics

Many Japanese employ foreign currency exchange to obtain foreign currency when they go overseas for sightseeing, business, etc. Foreign currency exchange is also employed 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 includes hoteliers, travel agencies, and secondhand dealers. They deal with foreign currency exchange as a sideline for the convenience of customers in their main business (see table 12).

By physically bringing criminal proceeds overseas, it is possible to lower the possibility of detection of the proceeds, punishment, confiscation, etc. After exchanging criminal proceeds to foreign currency, it is also possible to use the proceeds while lowering such possibility. Furthermore, foreign currency exchange has the characteristics of handling cash which is high in liquidity and anonymity, and the capability of physically changing the appearance of criminal proceeds and integrating a lot of bills of small denominations into a small number of bills of high denominations.

In Japan, license or registration is not required to operate foreign currency exchange business. Anyone can conduct the business. In the third round Mutual Evaluation by the FATF, such a situation was pointed out as deficiency. New "40 Recommendations" of the FATF (Recommendation 26) requires that "Businesses providing a service of currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national AML/CFT requirements as mentioned above.

Table 12 [Transactions by Foreign Currency Exchange Operators (March, 2018)]

Reporters	Number of reporters (Note 3)	Number of transactions	Transaction value (million yen)	Value per transaction (1,000 yen)
Deposit-taking institutions				
Major banks	4	315,261	23,090	73.3
Regional banks	91	215,774	13,510	62.7
Shinkin banks	126	5,420	548	101.2
Foreign banks	27	1,025	6,012	5865.4(Note 4)
Other deposit-taking institutions (Note 2)	8	42,024	2,478	59.0
Excluding deposit-taking institutions				
Funds transfer service/credit card business	14	217,685	11,217	51.6
Hoteliers	44	4,226	126	29.9
Travel agencies	27	45,829	2,416	52.8
Secondhand dealers	42	54,923	3,780	68.9
Service providers related to airport	3	183,638	5,703	31.1
Large-scale retailers	3	394	10	25.4
Others	102	72,924	6,488	89.0
Total	491	1,159,123	75,378	65.1

Note 1: Data from the Ministry of Finance
2: The Shinkin Central Bank, credit associations, Japan Post Bank, and other banks
3: Number of operators that conducted foreign currency exchange transactions more than one million yen for business in February 2018 and then conducted a foreign currency exchange transaction(s) in March 2018 (pursuant to the Foreign Exchange and Foreign Trade Act, if the total transaction volume has exceeded one million yen in a month, performance in the following month shall be reported.)
4: Value per transaction is large because some banks procure/buy foreign currency with other financial institutions.

(b) STRs

There were 2,750 STRs by foreign currency exchange operators from 2015 to 2017. Among cases exampled in "List of Reference Cases of Suspicious Transactions," major ones (and the number of reports) are as follows.

○ Currency exchange of large amounts of cash or traveler's checks (920 reports, 33.5%)
○ Cases suspected that a customer visits a particular shop or its neighboring shops several times a day or during a couple of days so that the amount of each transaction is slightly lower than the threshold for verification at the time of transactions (581 reports, 21.1%)

(c) Case

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

○ A case where an offender of murder attended with robbery overseas gained huge foreign currency from the crime, then converted it to Japanese yen through a third party

Meanwhile, the following is an example case abroad:

○ A case where a drug trafficking organization used unregistered foreign currency exchange operators to exchange drug proceeds to foreign currency

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

○ A 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 administrative authorities' supervision, etc. In addition, the Foreign Exchange and Foreign Trade Act requires foreign currency exchange operators, whose transaction volume is more than one 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 prepare and preserve verification records and transaction records when they make a transaction more than two million yen per transaction. The Act also requires foreign currency exchange 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result ofverification at the time of transactions the actual manner of the transactions and other relevant circumstances.

Moreover, in addition to the supervisory measures based on the Act, the Foreign Exchange and Foreign Trade Act stipulates that the competent administrative authorities may conduct on-site inspection of and issue a business improvement order to foreign currency exchange operators if necessary.

(b) Measures by competent administrative authorities

The Ministry of Finance has improved the Foreign Exchange Inspection Manual, which indicates focal points related to the development of internal control systems regardingverification 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 complete compliance with laws and regulations by foreign currency exchange operators, the Ministry prepares a pamphlet describing the outline of the reporting system, reporting procedures and the like for foreign currency exchange operators and publishes it on the homepage of the Ministry.

And, based on the result of on-site inspections and documentary research regarding compliance with laws and regulations and of risk control, the Ministry performs the risk assessment on respective operators from the viewpoints of the scale of currency exchange transactions, internal control system, existence of non-face-to-face transactions and, based on the result, provides the guidance and supervision corresponding to risks.

Furthermore, the Ministry holds briefing sessions for foreign currency exchange operators and, together with the National Police Agency, sends them a document that requires thorough implementation of verification at the time of transactions and making STRs. If the compliance of the Act on Prevention of Transfer of Criminal Proceeds and the Foreign Exchange and Foreign Trade Act turned out to be insufficient implementation during on-site inspection at operators, deficiencies would be pointed out and required to be improved.

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

These obligations and supervision are important to understand the actual state of foreign currency exchange and to prevent foreign currency exchange from being misused for ML/TF.

(c) Measures by industry organizations and business operators

Some foreign currency exchange operators make autonomous efforts against ML/TF beyond those required by regulations. These operators, mainly those who handle a large volume of foreign currency exchange, set lower threshold for verification at the time of transactions than a legal threshold. Other than that, they take measures to establish and strengthen their internal control systems. For example, they develop AML/CFT manuals, set up a division in charge, and provide training and internal audit. On the other hand, operators who handle lower volume tend to be modest in taking such measures.

The followings are recognized as examples of the risk assessment and of efforts for risk-based approach taken by business operators:

- ○ Cases where transactions for a certain amount are classified into high-risk transactions and, if such transactions occur, measures such as reporting to the headquarters and execution of necessary research are specified in internal regulations; and,
- ○ Cases where, considering the risk of large transactions being intentionally separated into multiple small transactions for the purpose of avoiding the verification at the time of transaction, the verification is conducted based on a threshold value which is independently specified internally, and results are entered into a database, and the existence of customers conducting transactions totaling a large amount is monitored.

C. Assessment of Risks

Foreign currency exchange can be a part of a measure to take out proceeds derived from crimes committed overseas and use them. Foreign currency exchange is usually carried out in cash which has high liquidity and can be possessed or transferred without information of the holder. From these characteristics, foreign currency exchange can be a useful measure for ML/TF.

Actually, there is a case where foreign currency which is criminal proceeds gained overseas was converted to Japanese yen through a third party who didn't know the actual circumstances. Considering a relevant situation, it is recognized that foreign currency exchange has risks to be misused for ML/TF.

Competent administrative agencies and operators are taking, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts are different by operators, 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 having the following aspects such as transaction conditions, customer types, etc. would be exposed to higher risks.

- ○ Transactions of large amounts of cash

- ○ Frequent transactions in a short period
- ○ Transactions suspected that the customer intentionally avoid verification at the time of the transactions
- ○ Transactions suspected that the customer acts on behalf of other people
- ○ Transactions related to currency etc., which was forged/stolen or suspected to be forged/stolen

(9) Financial Leasing Dealt with by Financial Leasing Operators

A. Factors of Risks

(a) Characteristics

Financial leasing is dealt with by a financial leasing operator, in the form of contracting with a company etc., (lessee) who intend 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 who intends to obtain facilities can make the payment on the installment plan for a certain period. Financial leasing has certain characteristics, such as existence of a supplier in addition to the contracting parties (i.e. a financial leasing operator and a lessee), and the relatively long leasing period. Due to those, financial leasing may be misused for ML/TF through, for example, a scheme where a lessee and a supplier in conspiracy make up fictitious financial leasing.

In addition, the Road Transport Vehicle Law (Act No. 185 of 1951) stipulates that no motor vehicles shall be driven if the name and address of the owner, principal place of use, etc., are not registered in the vehicle registration file managed by the Minister of Land, Infrastructure, Transport and Tourism. In effect most of the leased vehicles are registered ones, so the registration system is useful to mitigate the risks motor vehicle leasing has.

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

(b) STRs

There were 483 STRs by financial leasing operators from 2015 to 2017. Among cases exampled in "List of Reference Cases of Suspicious Transactions," major ones (and the number of reports) are as follows.

- ○ Transactions related to Boryokudan or its related parties (381 reports, 78.9%)
- ○ Transactions related to financial leasing suspected that a lessee etc., intend to defraud a financial leasing operator of money by concluding several leasing contracts based on the same facilities (so called "multiple leasing") (43 reports, 8.9%)
- ○ Transactions related to financial leasing suspected that a lessee and a supplier in conspiracy intend to defraud a financial leasing operator of money by pretending to install facilities (so called "empty leasing") (26 reports, 5.4%)

.

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 prepare and preserve verification records and transaction records when they conclude contracts. The Act also requires financial leasing 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances. Moreover, the Act also provides for supervisory measures by the competent administrative authorities, such as requiring the submission of reports and conducting on-site inspection.

(b) Measures by competent administrative authorities

The Ministry of Economy, Trade and Industry provides assistance, etc., to efforts by the following industry organizations to ensure the development of internal control system by business operators.

(c) Measures by industry organizations and business operators

Japan Leasing Association and 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 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, Japan Leasing Association executes the documentary research to member companies of the Association every year and executes the risk assessment for ML/TF, based on the results, etc., of such research.

C. Assessment of Risks

Although there were no arrests in money laundering cases in which financial leasing is misused, because finance leases have the characteristic of a lessee and a seller being able to conspire to conduct a transaction without realty, it is considered that finance leases are at risk of being misused for ML/TF.

Competent administrative agencies and operators are taking, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts are different by operators, 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 having the following aspects such as transaction conditions, customer types, etc. would be exposed to higher risks.

- ○ Financial leasing contracts suspected that the customer uses a fictitious or other person's name
- ○ Transactions related to financial leasing suspected that a lessee and a supplier in conspiracy intend to defraud a financial leasing operator of money by pretending to install facilities
- ○ Transactions related to financial leasing suspected that a lessee etc., intend to defraud a financial leasing operator of money by concluding several leasing contracts based on the same facilities

(10) Credit Cards Dealt with by Credit Card Operators

A. Factors of Risks

(a) Characteristics

Credit cards are widely used as the method for payment because they can be used in a timely manner, with simple procedures.

Credit cards could make it difficult to track criminal proceeds because a holder of criminal proceeds in cash can transform them into different kinds of property through a credit card.

Furthermore, by providing a credit card or credit card information to a third party, it is possible to make the third-party purchase products etc. Credit cards can be used all over the world, and some of them have a high usage maximum amount. Therefore, for example, if someone who intends to transfer funds provides a third party with a credit card and make him/her purchase a cashable product and the third party sells the product, it is actually possible to transfer funds, either in Japan or abroad.

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 of comprehensive credit purchases, in which operators are provided by a user with money corresponding to the payment for products etc., over two months or in a revolving form[*1]. As of the end of March, 2018, 259 operators were registered.

(b) STRs

There were 42,550 STRs by credit card operators from 2015 to 2017. Among cases exampled in "List of Reference Cases of Suspicious Transactions," major ones (and the number of reports) are as follows.

- ○ Transactions related to Boryokudan or its related parties (13,981 reports, 32.9%)
- ○ Credit card contracts suspected that the customer uses a fictitious or other person's name (12,459 reports, 29.3%)
- ○ Cases suspected that a person who is not a true card holder uses the credit card (7,447 reports, 17.5%)

(c) Case

The following are example cases of misuse of credit cards for money laundering:

- ○ A case where a Boryokudan-related person accepted a credit card obtained through fraud by 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 falsifying ID
- ○ A case where a shop owner operating a loam shark 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.

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 prepare and preserve verification records and transaction records when they conclude contracts. The Act also requires operators 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, through taking account of the contents of this risk assessment report and a comparison with the manner of ordinary transactions and the like, in

---

*1 In a revolving form, 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).

addition to the result of verification at the time of transactions, the actual manner of the transactions and other relevant circumstances.

In addition to the supervisory measures based on the Act, the Installment Sales Act stipulates that the competent administrative authorities can require 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 guidelines for comprehensive credit purchase intermediaries, focal points include execution of the obligation to conductverification at the time of transactions and to file STRs under the Act on Prevention of Transfer of Criminal Proceeds.

(b) Measures by competent administrative authorities

The Ministry of Economy, Trade and Industry also perform documentary research to grasp the actual situation of compliance with laws and regulations and risk control by business operators and provide guidance and supervision, etc., corresponding to risks of respective business operators based on information obtained by such research and orders.

(c) Measures by industry organizations and business operators

Japan Consumer Credit Association has made self-regulating rules which require member companies to conduct verification at the time of transactions and STRs. The Association also supports AML/CFT measures taken by operators through providing training on making STRs, along with introduction of a system which enables member companies to register card holder information with credit bureaus designated by the Minister of Economy, Trade and Industry based on the Installment Sales Act. When operators receive application for concluding or renewing a contract, they can refer to the system to examine whether any suspicious situations exist, for example, whether a person has applied for several credit cards in a short period.

Business operators also make voluntary efforts. For example, they set a usage maximum amount on each card holder after strict admission/renewal examination, screen out transactions that are considered at 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 meeting with law enforcement authorities.

The followings are recognized as examples of the risk assessment and of efforts for risk-based approach taken by business operators:

- ○ A case 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 the holder of the card is given a telephone call to check the content of use or the user; and,
- ○ A case where the increase of the availability of a credit card is not authorized in principle until a year elapses after the application to mitigate risks by a person attempting money laundering using a contract

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/her purchase products. Considering a relevant situation, it is recognized that credit cards have risks to be misused for ML/TF.

Competent administrative agencies and operators are taking, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts are different by operators, 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 having the following aspects such as transaction conditions, customer types, etc. would be exposed to higher risks.

- ○ Credit card contracts suspected that the customer uses a fictitious or other person's name
- ○ Transactions related to a customer who frequently purchases large amounts of cash equivalent, such as gift cards, by the use of credit cards
- ○ Cases suspected that a person who is not a true card holder uses the credit card

(11) Real Estate Dealt with by Real Estate Brokers

A. Factors of Risks

(a) Characteristics

Real estate has high value and can be exchanged to a large amount of cash. In addition, result of evaluation or real estate 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 customary price. It is also possible to obscure source of funds or beneficial ownership of real estate by purchasing it under a fictitious or other person's name.

Among real estate products, building lots and buildings are especially valued and actively traded in Japan.

Business operators who handle transactions of these properties are subject to relevant laws and regulations as Real Estate Brokers (Brokers). In order 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 Building Lots and Buildings Transaction Business Act (Act no. 176 of 1952). There were approximately 123,782 brokers as of the end of March 2018. In 2016, the annual amount of sales were about 43 trillion yen, and the annual number of transactions which were registered and noticed to the real estate information network designated by the Minister of Land, Infrastructure, Transport and Tourism was approximately 180,000. Business scale varies significantly across Real Estate Brokers. While there are major Brokers who handle more than thousands of transactions a year, there also exist small and medium-sized Brokers, such as a private business who conduct community-based operation. The latter gets a majority.

(b) STRs

There were 24 STRs by brokers from 2015 to 2017. Among cases exampled in "List of Reference Cases of Suspicious Transactions," major ones (and the number of reports) are as follows.

○ Purchase of building lots or buildings in large amount of cash. (6 reports, 25.0%)
○ Unusual transactions or transactions related customers who show unusual behavior or actions, based on the knowledge and experience of a company's own employees (6 reports, 25.0%)

(c) Case

The following are example cases of misuse of 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 is an example case abroad:

○ A case where drug traffickers bought real estate by the use of drug proceeds and their friend's name, and used the real estate for living and drug manufacturing

and so on. Meanwhile, the following is an example case 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 of building lots and buildings or conduct intermediary or agency service thereof. The Act also requires Real Estate Brokersto 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

Furthermore, in addition to the supervisory measures based on the Act, the Real Estate Brokerage Act provides for supervisory measures by the competent administrative 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 office of Brokers must keep books which record 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 lots and buildings business.

(b) Measures by competent administrative authorities

The Ministry of Land, Infrastructure, Transport and Tourism also performs documentary research or hearings to grasp the actual situation of compliance with legal regulations and risk control by business operators and provide the guidance and supervision, etc., corresponding to risks of respective business operators based on information obtained by such research and orders.

(c) Measures by industry organizations and business operators

Furthermore, the "Liaison Council for Prevention of Transfer of Criminal Proceeds and Prevention of Damage by Anti-social Forces in Real Estate Business" makes efforts to secure effective implementation of the Act on Prevention of Transfer of Criminal Proceeds, including information sharing efforts. For example, this council arranged an agreement on Brokers' developing a management system to prevent from being misused for ML/TF and damage by anti-social forces, and distributes leaflets for announcement and education.

The followings are recognized as examples of the risk assessment and of efforts for risk-based approach taken by business operators:

- ○ A case where information on transactions with customers for whom transactions were cancelled or transactions were not achieved for any reason in the past is made into a database to be shared by all employees of the company and, if any subsequent transactions with such customers occur, measures to strengthen customer control or to reject transactions are taken; and,
- ○ A case where, in order not to overlook transactions with Anti-social Forces, an operator independently prepares a checklist regarding characteristics of speech and behavior of Anti-social Forces and utilizes the checklist for customer control

C. Assessment of Risks

Real estate has high value and can be exchanged to large cash. Furthermore, it is possible for offenders to transfer criminal proceeds by for example, paying more than customer price. From these aspects, real estate can be a convenient instrument for ML/TF.

Actually, there are some cases where criminal proceeds from prostitution or fraud were used to buy real estate. Considering a relevant situation, it is recognized that real estate has risks to be misused for ML/TF.

Competent administrative agencies and operators are taking, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts are different by operators, 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 having the following aspects such as transaction conditions, customer types, etc. would be exposed to higher risks.

- ○ Transactions of large amounts of cash

○ Transactions suspected that they were conducted under a fictitious or other person's name

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

A. Factors of Risks

(a) Characteristics

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

In cases where a person impose or exports by carrying precious metals weighing more than 1 kilogram, they are required to make a prior declaration to Customs under the Foreign Exchange and Foreign Trade Act and the Customs Act (Act No. 61 of 1954). However, in recent years, smuggling of gold bullion has been growing. In administrative year[*1] 2017, the number of processed cases (notifications and indictments) of gold smuggling was 720, a record high, and the value of tax evasion was approximately 1,500 million yen, also a record high (see tables 13 and 14).

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, to 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, the methods of smuggling has been seen more sophisticated and small-sized by processing the gold or changing its shape to conceal it in a body cavity or clothing, etc. Likewise, there has been a trend in the diversification of smuggling methods by using air passengers, air cargo, and international postal mail, etc., the dispersion of entrance airport to local airports, and so on. Hong Kong and Korea are the major place of shipments for smuggling. In addition, a circularscheme to repeat the acquisition of criminal proceeds is observed in which gold bullion purchased abroad from criminal proceeds obtained by the above-mentioned smuggling is smuggled into Japan again and sold in purchasing shops in Japan. In the background, the actual situation of the involvement of domestic and overseas syndicates, such as Korean illicit dealers, Boryokudan-related persons, and so on, is recognized.

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.

Table 13 [Changes in the number of processed cases of gold bullion smuggling (administrative year 2015 to 2017)]

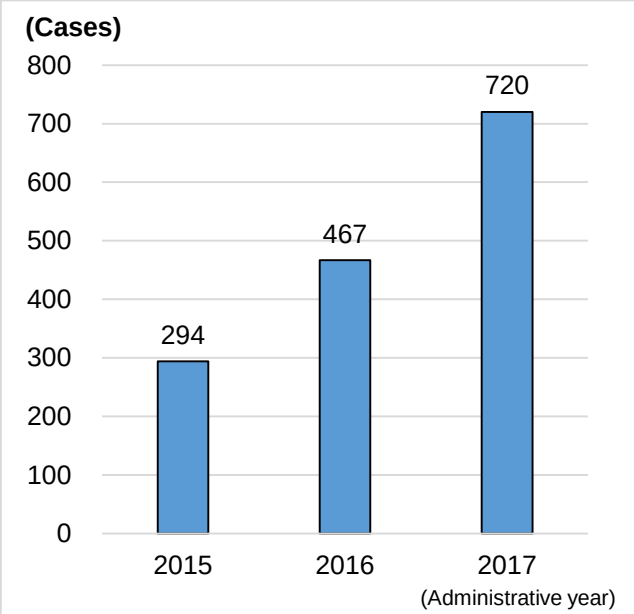
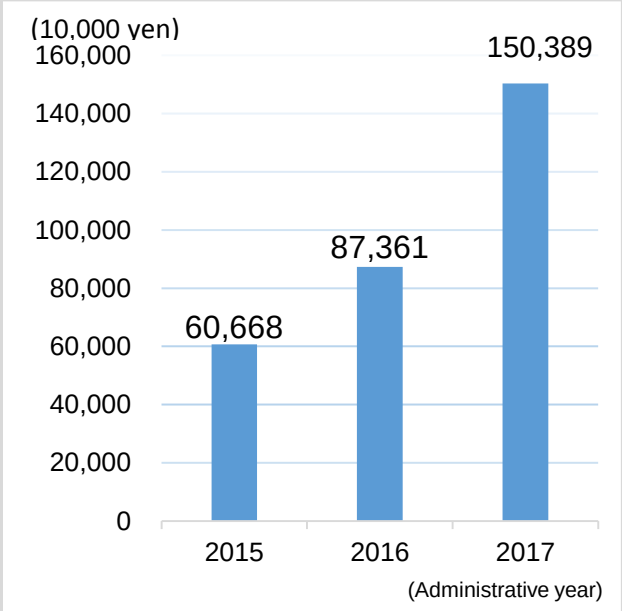


Table 14 [Changes in the tax evasion amount in cases of gold bullion smuggling (administrative year 2015 to 2017)]



*1 The period from July 2017 to June of the following year.

(b) STRs

There were 183 STRs by dealers in precious metals and stones from 2015 to 2017. Among cases exampled in "List of Reference Cases of Suspicious Transactions," major cases (and the 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 their own employees (91 reports, 49.7%)
- ○ Purchases by the large amount of cash (17 reports, 9.3%)
- ○ The large amount of purchase or sales which is not proportionate to the customer's income, and assets, etc., (17 reports, 9.3%)

(c) Case

The following are example cases of misuse of precious metals and stones for money laundering in Japan.

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

These transactions were conducted with an increased level of anonymity, by impersonating to another person or falsifying identification data, etc. through the presentation of forged ID at the time of the conclusion of contracts on perchase. Besides in abroad, there is

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

Which shows the actual situation that precious metals and stones are misused for money laundering, due to their high anonymity and the ease of cashing 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 two million yen in cash. The Act also requires dealers in precious metals and stones to file STRs when property received in the transactions is suspected to be from criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

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 administrative authorities

The Ministry of Finance developed the "Stop Gold Smuggling" emergency countermeasures in November 2017 as a comprehensive countermeasures regarding the strengthening of inspection and punishment against the smuggling of gold bullion and has been promoting various countermeasures under a cooperative system with concerned ministries and agencies, including the amendment to relevant laws and regulations; which includes the complete fulfillment of obligations for 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 or hearings to grasp the actual situation of compliance with laws and regulations and risk control by operators and provide the guidance and supervision, etc., corresponding to risks of respective business operators based on information obtained by such research. Specifically, since a violation in which more than

one operator of gold bullion transactions 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 by cash during a short period was revealed by actual situation research. So the Ministry rendered the administrative guidance to these operators in April 2018, the content of which was as follows:

○ To report suspicious transactions promptly;
○ For the purpose of preventing the recurrence of violations, to take measures to further strengthen education and training to employees and to perform obligations of verification of transactions including maintenance and review of regulations reliably

and so on.

In addition, the Ministry makes efforts to renders the administrative guidance including the issuance of guidance documents to operators who are considered to have insufficient understanding of the risk control, etc., and to hold seminars for the industry. Furthermore, the Ministry tries to ensure the complete practice to perform obligations by indicating an URL for accepting questions concerning the Act on its homepage to accept questions from operators.

(c) Measures by industry organizations and business operators

For the purpose of preventing the purchase of smuggled gold bullion, the Japan Gold Metal Association executes voluntary regulations on gold bullion transactions by requesting operators to check tax payment receipts at customs for gold bullion purchased in foreign countries.

The Japan Jewelry Association tries to improve the level of understanding of operators on ML/TF, by preparing and distributing leaflets containing an outline of the Act on Prevention of Transfer of Criminal Proceeds and the content of obligations required for operators, by holding briefing sessions for countermeasures towards ML/TF, and by establishing a homepage dedicated to the improvement of understanding.

The antique dealers industry organization tries to promote complete understanding and thorough practice of countermeasures for ML/TF, by preparing a manual organizing the manner of performing obligations under relevant laws and regulations (the Act on Prevention of Transfer of Criminal Proceeds and the Antique Dealings Act) for the purpose of promoting efforts to prevent ML/TF. 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 for members, home page, etc., for members. Furthermore, operators are making efforts to establish and strengthen their internal control systems to prevent money laundering by regularly having external audits by acquiring international industry certifications, maintaining regulations and manuals, and conducting regular training.

C. Assessment of Risks

Precious metals and stones have high value. They are distributed all over the world. It is easy to exchange to cash or carry with. In addition, it is difficult to track distribution channels and locations after transactions with 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 money laundering.

Actually, there are cases where offenders pretended to be another person and bought precious metals with cash derived from crimes. Considering a relevant situation, it is recognized that precious metals and stones have risks to be misused for ML/TF.

Taking into account the crimes committed in relation to gold bullion in recent years, it is believed that the degree of risk in which gold bullion is misused for money laundering is increasing. Against such degree of risks, competent administrative agencies and operators execute risk-mitigating measures as mentioned above in addition to statutory measures, and, by these measures, the effect of risk-mitigating measures are shown to a certain extent as seen in the facts that the recognition of operators is improved and the number of suspicious transaction reports have substantially increased.

However, the level of these efforts are different by operators, 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 having the following aspects such as transaction conditions, customer types, etc. would be exposed to higher risks.

- ○ Transactions of large amounts of cash
- ○ Transactions of frequent purchases resulting in a large amount, even if the purchase amount at the time is small
- ○ Purchase or sales with high value which are not proportionate to the customer's income, assets, etc.
- ○ Transactions suspected that identification documents, etc., provided at the time of customer identification might be falsified
- ○ Transactions suspected that customers sell precious metals etc., but ownership is suspicious

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

A. Factors of Risks

(a) Characteristics

In postal receiving service business, service providers consent to use their 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 the use of the service, customers can announce a place where they do not actually live as their address and receive mail. There are cases where postal receiving service providers are misused as a delivery address of defrauded money etc., in specialized fraud etc.

During the investigations related to specialized fraud, etc., it was suspected that, in 6 cases, suspicions ofpostal receiving service providers were violating the obligation of verification at the time of transactions were recognized. As a result, the National Public Safety Commission required the submission of reports from the said 6 postal receiving service providers in 2017. Specific cases of violation identified through the submitted reports are as follows:

○ Neglected to verify the customers' purposes of transactions, their occupations, etc.
○ Neglected to verify the beneficial ownership and control of corporate customers
○ Neglected to send transaction documents by registered mail in non-face-to-face transactions
○ Neglected to prepare or keep verification records

and so on.

(b) STRs

There were 32 STRs by postal receiving service providers from 2015 to 2017. Among cases exampled in "List of Reference Cases of Suspicious Transactions," major ones (and the number of reports) are as follows.

○ Transactions related to customers who show unnatural behavior or attitude in the process of contract which was found based on the knowledge and experience of staff (7 reports, 21.9%)
○ Contracts suspected to be made in the name of fictitious or other person's name (3 reports, 9.4%)

(c) Case

The following are example cases of misuse of postal receiving service for money laundering:

○ A case where proceeds derived from false bill fraud was forwarded to several locations including a postal receiving serve provider then received by the offender
○ Cases where repaid loans 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 postal receiving service providers 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances. Furthermore, the Act provides for supervisory measures by the competent administrative authorities, such as requiring the submission of reports and conducting an on-site inspection.

(b) Measures by competent administrative authorities

Furthermore, in order to ensure thorough postal receiving service providers' compliance, the Ministry of Economy, Trade and Industry holds briefing sessions for them and explain the outline of the Act on Prevention of Transfer of Criminal Proceeds and important points of their obligation under the Act and sends documents to raise awareness on matters to be verified at the time of transaction to postal receiving service providers. In addition, the Ministry sends brochures to inform postal receiving service providers of verification at the time of transactions and it explains the Act on its website.

Furthermore, the Ministry executed on-site inspection, issued rectification orders and provided 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 tried to raise awareness on the performance obligations based on the Act and issue 6 rectification orders to postal receiving service providers during the period from 2015 to 2017, the content of which was as follows:

○ To improve the company regulation to smoothly proceed the procedure regarding the in-company training on the Act on Prevention of Transfer of Criminal Proceed and other procedure related to the Act
○ To review work related to verification at the time of transaction and to the preparation and retention of verification records

and so on. As a result, some providers could not implement the rectification orders, gave up, and discontinued business.

In addition, the Ministry performs documentary research or hearings to grasp the actual situations of compliance with laws and regulations and of risk control by operators and provides the guidance and supervision, etc., corresponding to risks of respective operators based on information obtained by such research and hearings and verification results of violation cases, etc.

(c) Measures by operators

The following are recognized as examples of the risk assessment and of efforts for 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

C. Assessment of Risks

Postal receiving service is misused to provide locations to which proceeds derived from crimes including frauds and sales of illegal goods are sent. If falsified customer identification data are provided to conclude service contract, the principal of ML/TF, or ownership of criminal proceeds can be unclear. Therefore, postal receiving service can be an effective instrument for ML/TF.

Actually, there are cases where offenders made contract with postal receiving service providers in a fictitious name and made providers receive criminal proceeds for concealment. Considering a relevant situation, it is recognized that postal receiving service has risks to be misused for ML/TF.

Moreover, postal receiving service providers' neglect to fulfill their duties under laws and regulations as mentioned above due to deficiencies of their internal control systems may increase risks involved in postal receiving service.

Against such degree of risks, competent administrative agencies and operators take, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts are different by operators, 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 having the following aspects such as transaction conditions, customer types, etc. would be exposed to higher risks.

○ Transactions suspected that customers might use the service to disguise the company's actual state
○ Transactions with a customer who plans to make contracts of postal receiving service using multiple companies' names

- ○ Transactions with customers who often receive a large amount of cash
- ○ Transactions with customers suspected of having concluded contracts in fictitious or other persons' names

(14) Telephone Receiving Service Dealt with by Telephone Receiving Service Providers

A. Factors of Risks

(a) Characteristics

Telephone receiving service providers consent to use their telephone number as a customer's telephone number, provide service to receive the call to the customer's telephone number, and transmit the content to the customer.

By the use of the service, customers can announce a telephone number which is different from that of their home or office as their telephone number, and can receive a telephone call using the provider's number. Because of these characteristics, telephone receiving services are misused in specialized fraud etc.

(b) STRs and Case

We have not seen a cleared money laundering case where telephone receiving service was misused in recent years. However, there are cases where a telephone receiving service was misused for making a principal of money laundering or ownership of criminal proceeds unclear in, for example, a fraud case where a victim was claimed charges for application to public grants. The number of STRs by telephone receiving service providers was one between 2015 and 2017.

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 prepare and preserve verification records and transaction records when they make service contracts. The Act also requires telephone receiving service providers 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances. In addition, the Act provides for supervisory measures by the competent administrative authorities, such as requiring the submission of reports and conducting on-site inspection.

(b) Measures by competent administrative authorities

In order to ensure telephone receiving service providers' compliance, the Ministry holds briefing sessions for them and explains the outline of the Act on Prevention of Transfer of Criminal Proceeds and important points of their obligation under the Act. The Ministry of Internal Affairs and Communications also explains the Act on its website.

The Ministry also performs documentary research or hearings to grasp the actual situation of compliance with laws and regulations and risk control by business operators and provide the guidance and supervision, etc., corresponding to risks of respective business operators based on information obtained by such research and orders.

C. Assessment of Risks

We have not seen any cases of arrest for money laundering recently 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 make the principal of ML/TF, and the owner of criminal proceeds unclear, it is considered that telephone receiving services have a risk of being misused for ML/TF.

Competent administrative agencies are taking, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts are different by operators, 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.

(15) Telephone Forwarding Service Dealt with by Telephone Forwarding Service Providers

A. Factors of Risks

(a) Characteristics

Telephone forwarding service providers consent to use their telephone number as a customer's telephone number and provide service to automatically forwards the call to or from the customer to the telephone number designated by the customer.

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

To operate a business as a telephone forwarding service provider, providers should make an application stipulated in the Telecommunications Business Act (Act No. 86 of 1984). As of the end of March 2018, there were 819 companies which had made an application to provide telephone forwarding service.

Also, in recent years, IP telephones, which propagate voice data over Internet lines, are becoming popular, making it possible for even a mobile phone terminal such as a smartphone without a telephone number to utilize telephone service using a special application. An actual circumstance in which a telephone transfer service using a new technology that can display the telephone number of a landline telephone such as 03 number on the other party's telephone by transmitting from a mobile phone terminal, etc., without a telephone number and by going through switching equipment or a cloud PBX provided by a provider is misused in special kinds of fraud, etc., has been recognized. The method of deception is changing from the misuse of rental mobile phones in the past.

Actually, the number of reports from prefectural police departments to the National Public Safety Commission reporting that such services are used for crimes including special kinds of fraud and that suspected violation of obligations of verification at the time of transaction is recognized on telephone transfer service providers have been increasing since 2017.

Based on the above-mentioned actual circumstance, the National Public Safety Commission collected 10 reports based on the Act on Prevention of Transfer of Criminal Proceeds until October 1, 2018. Specific cases of violation identified through the submitted reports are as follows:

○ Neglected to verify the customers' purposes of transactions, their occupations, etc.
○ Neglected to conduct the verification at the time of transaction by valid principal identification documents
○ Neglected to prepare or keep verification records

and so on.

(b) STRs and Case

STRs by telephone forwarding service providers were not made from 2015 to 2017.

And, the following is an example case of misuse of telephone forwarding service for money laundering:

○ There cases, etc. where, in concealment of criminal proceeds derived from the sale of obscene DVDs, more than one telephone forwarding service contracted under another person's name is misused for communication with customers as a means to make the owner of the criminal proceeds unclear.

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 prepare and preserve verification records and transaction records when they make service contracts. The Act also requires telephone forwarding service providers 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

Furthermore, in addition to the supervisory measures based on the Act, the Telecommunications Business Act provides that the competent administrative authorities may require the submission of reports from and conduct on-site inspection of telecommunication business operators as far as is necessary in order to enforce this act.

(b) Measures by competent administrative authorities

Furthermore, in order to ensure thorough telephone receiving service providers' compliance, the Ministry of Internal Affairs and Communications holds briefing sessions for them and explain the outline of the Act on Prevention of Transfer of Criminal Proceeds and important points of their obligation under the Act. In addition, the Ministry sends brochures to inform telephone forwarding service providers of verification at the time of transactions and it explains the Act on its website.

Furthermore, based on the statement of opinion on the basis of results of the above-mentioned report collection by the National Public Safety Commission, the Ministry of Internal Affairs and Telecommunications plans to execute report collection, etc., to the operators in question based on the Act on Prevention of Transfer of Crime Proceeds and to provide individual and specific guidance, etc.

Furthermore, the Ministry of Internal Affairs and Telecommunications plans to perform documentary research to grasp the actual situation of compliance with laws and regulations and risk control by operators and subsequently to plan a hearing and provide the guidance and supervision, etc., corresponding to risks of respective business operators based on information obtained by such research and hearing.

C. Assessment of Risks

Through telephone forwarding services, customers can give their business a false appearance and can make the principal of ML/TF, or ownership of criminal proceeds unclear. Considering this relevant situation, it is recognized that telephone forwarding services have the risk of being misused for ML/TF.

Moreover, telephone forwarding service providers' neglecting to fulfill their duties under laws and regulations as mentioned above due to deficiencies of their internal control systems may increase the risks involved in telephone forwarding services.

Against such risks, competent administrative agencies try to raise awareness for the performance of statutory obligations by operators and to mitigate the degree of risks by guidance and supervision including the above-mentioned risk-mitigating measures and administrative response.

However, the level of these efforts are different by operators, and operators for which effective risk-mitigating measures corresponding to risks are not taken may suffer risk of misuse for ML/TF, and may influence the risk for the type of business as a whole.

(16) Legal/Accounting Service Dealt with by Legal/Accounting Professions[*1]

A. Factors of Risks

(a) Characteristics

There are lawyers, judicial scriveners, and certified administrative procedures legal specialists who possess legal expertise as professions. There are certified public accountants and certified public tax accountants who possess accounting expertise as professions (Hereinafter referred to as "legal/accounting professions").

Lawyers provide legal services at the request of a client or other person concerned. A lawyer must be registered in the roll of attorneys kept at Japan Federation of Bar Associations (hereinafter referred to as "JFBA") and must belong to a bar association that is established in jurisdiction of each district court. As of the end of March, 2018, 40,066 lawyers, 8 Okinawa special members, 408 foreign lawyers, 1,134 legal profession corporations and five foreign legal profession corporations are registered.

Judicial scriveners provide services related to registration on behalf of client, consult about registration, and engage in the legal representation in summary court, etc. A judicial scrivener must be registered in the judicial scrivener roster kept in Japan Federation of Shiho-Shoshi Lawyer's Associations. As of the end of March 2018, 22,516 judicial scriveners and 662 judicial scrivener corporations are registered.

Certified administrative procedures legal specialists prepare documents to be submitted to a public agency and documents relating to rights, duties or the certification of facts at the request of client. Other than that, certified administrative procedures legal specialists can carry out procedures as an agent to submit documents to a public agency. A certified administrative procedures legal specialists must be registered in the certified administrative procedures legal specialists registry kept in Japan Federation of Certified Administrative Procedures Legal Specialists Associations. As of the end of March, 2018, 46,915 certified administrative procedures legal specialists and 595 certified administrative procedures legal specialist corporations are registered.

Certified public accountants shall make it their practice to audit or attest 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 2018, 30,350 certified public accountants, 2 foreign certified public accountants, and 229 audit firms are registered.

Certified public tax accountants represent clients for filing, application, request, report, statement under laws regarding tax payment to tax agencies and prepare tax forms and consult about tax. Other than that, as incidental business of the mentioned above, they prepare financial forms, keep accounting books on client's behalf, and provide any services related to finance. A certified public tax accountant must be registered in the roll of certified public tax accountants kept in Japan Federation of Certified Public Tax Accountants' Associations. As of the end of March, 2018, 77,327 certified public tax accountants and 3,727 certified public tax accountants' corporations are registered.

As mentioned above, legal/accounting professions possess expertise regarding law and accounting. They have good social credibility and are involved in various transactions.

However, for those who attempt the ML/TF, legal/accounting professions are useful because they have indispensable expertise in legal/accounting fields to manage or dispose property according to the purpose. At the same time, they can make up legitimate appearance in transactions and asset management by the use of high social credibility.

Furthermore, FATF suggests that, as the regulations on ML/TF, are effectively executed to banks,

---

*1 Legal/accounting professions mean those who listed in Article 2, Paragraph 2, Item 43 (lawyer or legal profession corporation), Item 44 (judicial scrivener or judicial scrivener corporation), Item 45 (certified administrative procedures legal specialists or certified administrative procedures legal specialists 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.

etc., persons attempting to conduct ML/TF, come to commit 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 transactions, instead of ML/TF, through banks.

(b) Case

The following are example cases of misuse of legal and accounting services for money laundering in Japan:

- ○ A case where a loan shark asked a certified administrative procedures legal specialist to provide service for incorporation on behalf of them, set up a shell company, deceived financial institutions to open an account of 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 was used for accounting treatment of proceeds derived from frauds and gambling in order to disguise them as legitimate business profits

Meanwhile, the following is an example case abroad:

- ○ A case where an illicit dealer of drugs disguised proceeds derived from drug crime as a compensatory money paid by a purchaser of a building who was an accomplice, a lawyer who knew nothing about the circumstances was utilized as the agent for the sale and purchase of the building

and so on. An actual circumstance exists in which persons attempting to conduct money laundering utilize legal and accounting related services to disguise acts to conceal criminal proceeds as a legitimate transaction.

B. Measures to Mitigate Risks

(a) Statutory measures

The Act on Prevention of Transfer of Criminal Proceeds requires legal/accounting professions, 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 administrative authorities, such as requiring the submission of reports and reference materials from and conducting on-site inspection of legal and accounting experts (excluding lawyers).

Concerning lawyers, JFBA set rules and regulations which stipulate duty of lawyers, such as verification of client identity with regard to certain transactions, retention of records, and avoiding acceptance of request if there is any suspicion of being abused for ML/TF. Furthermore, in 2018 JFBA's rules and regulations were amended to require individual lawyers to submit annual report in regard to varification of client identity and retention of records.

(b) Measures by competent administrative authorities and self-regulated organization

Associations of each profession also make efforts to promote AML/CFT measures, for example, by developing regulations, preparing materials concerning duties, providing training, etc.

In addition, the JFBA encourages lawyers to understand the risks associated with their services by analyzing risks unique to their services based on hearings with major law firms, the content of annual reports or others and by publishing the results in the JFBA Journal.

Also, the Japan Federation of Shiho-Shoshi Lawyer's Association performs documentary quetionare of Shiho-Shoshi lawyers to check their compliance with the Act on Prevention of Transfer of Criminal Proceeds, and the Japan Federation of Certified Administrative Procedures Legal Specialists Associations performs documentary quetionare of certified administrative procedures legal specialists to check their compliance with the Act on Prevention of Transfer of Criminal Proceeds, and the Japanese Institute of Certified Public Accountants conducted survey on certified public accountants and audit firms to check their compliance with the Act on Prevention of Transfer of Criminal Proceeds every year, and the Ministry of Finance performs hearings with certified tax accountants about their compliance with the Act on Prevention of Transfer of Criminal Proceeds every year.

Through this research, the understanding of risks of ML/TF, is promoted among experts.

C. Assessment of Risks

Legal/accounting professions have high expertise about 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 affairs by legal/accounting professions are misused to disguise concealment of criminal proceeds as legitimate transaction. Considering a relevant situation, it is recognized that when legal/accounting professions conduct following transaction on behalf of clients, the service has risks to be misused for ML/TF.

○ Acts or procedures concerning buying and selling of building lots and buildings
Real estate has high value, it is easy to convert to a large amount of cash, and the value lasts long. Result of evaluation 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 to for ML/TF by paying the price padded against the appropriate value. On top of that, because sales transactions of real estate require complicated procedures, such as boundary setting and registration of a transfer of ownership, the relevant expertise is indispensable. Offenders can conduct transfer of criminal proceeds easier by performing the complicated procedures with the help of legal/accounting professions, who possess expertise and social credibility.

○ Acts or procedures concerning the establishment or merger of companies, etc.
Using the scheme of companies and other legal persons, cooperatives and trusts, they can make their assets independent of themselves. It means, for example, a huge amount of asset can be transferred under the name of business and offenders can hide the beneficial ownership or source of property without difficulty. These aspects generate the risk misused for ML/TF. On top of that, legal/accounting professions have expertise that is indispensable in organization, operation, and management of companies, etc., as well as social credibility. Offenders can conduct transfer of criminal proceeds easier by carrying out the act or procedures regarding establishment of company with the help of legal/accounting professions.

○ Management or disposition of cash, deposit, securities and other assets
Legal/accounting professions have expertise and valuable social credibility which are indispensable to store and sell assets or use the said assets for the purchase of other assets. When offenders manage or dispose asset with the help of legal/accounting professions, they can transfer of criminal proceeds without difficulty.

Competent administrative agencies and operators are taking, in addition to statutory measures, the above-mentioned risk-mitigating measures against these risks.

However, the level of these efforts are different by operators, and operators for which effective risk-mitigating measures corresponding to risks are not taken may suffer risk of misuse for ML/TF, and may influence the risk for the type of business as a whole.

2. Products and Services Utilizing New Technology, Which Requires Further Examination of Actual State of Use etc. (Electronic Money)

(1) Present Situation

The average usage amount of electronic money per household a month in Japan increased from 16,382 yen in 2015 to 17,644 yen in 2017. Meanwhile, the proportion of households which used electronic money worth more than 10,000 yen increased from 21.9% in 2015 to 24.6% in 2017. In Japan, the use of electronic money has spread in the past few years (see tables 15 and 16).

Seeing "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 that the value is recorded in computer servers etc.) that are issued in advance for value equivalent and used for purchase or leasing of goods or the receipt of provision of services from the issuer etc. Prepaid Payment Instruments is mainly used for specified services or at member shops for retail payment with small amount of value.

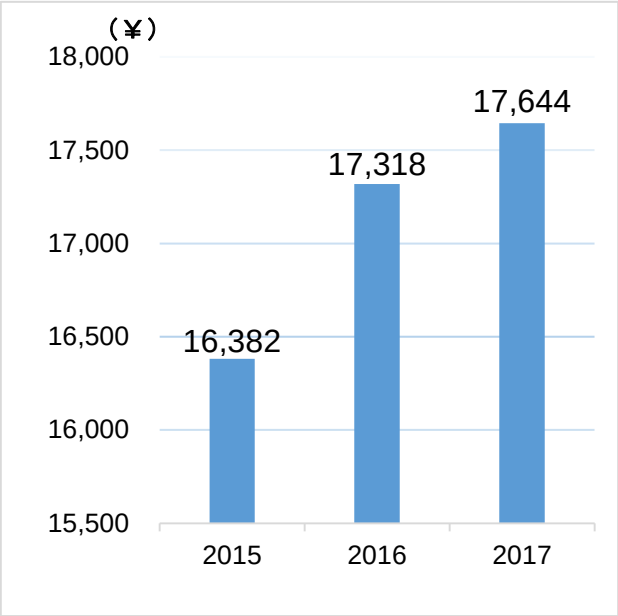
Prepaid Payment Instruments includes "own business type," which is used for payment to issuer only and "third-party business type," which is used for payment at member shops, too. The Payment Services Act requires issuers of Prepaid Payment Instruments for Third-Party Business to be registered with the competent authorities and issuers of Prepaid Payment Instruments for Own Business having unused balance exceeding designated threshold to notify to the competent authorities. The Act also sets many regulations, such as various reporting obligations, obligation of security deposits for issuance, management of member shops (measure to ensure that commodities are not against public order or morals), and prohibition of refund of Prepaid Payment Instruments in principle to ensure that appropriate service of Prepaid Payment Instruments should be implemented.

In Prepaid Payment Instruments, money value is changed to electromagnetic record and stored in IC chip or servers on network. The instruments have excellent transportability. Furthermore, in many cases, customers don't have to provide customer identification documents. Customer verification is often completed through only declaration of the customer's name and birth date on issuance. Because of these characteristics, Prepaid Payment Instruments have high anonymity. IC card 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 the business, users cannot freely withdraw funds with respect to the charge value. [*1] Furthermore, many issuers of Prepaid Payment Instruments voluntarily set the upper limit of charging and usage is limited to small value payment at specified member shops.

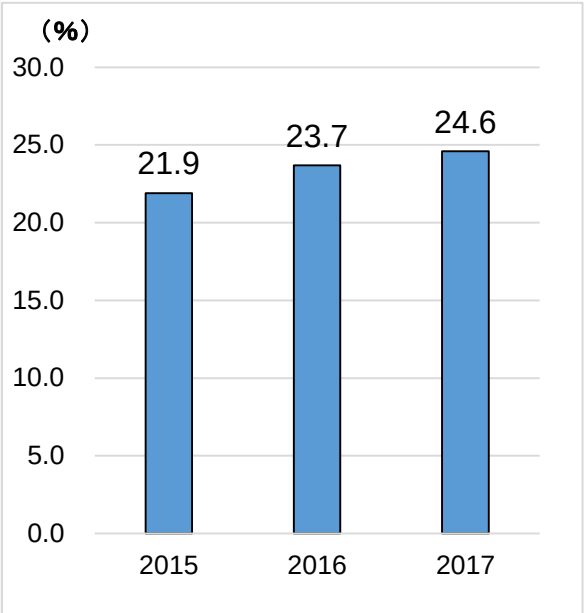
*1 Issuers of cards using the pre-paid payment methods whereby withdrawal or remittance is possible up to the charged value are equivalent to funds transfer service providers under the Payment Services Act, so they are designated as specified business operators under the Act on Prevention of Transfer of Criminal Proceeds. Therefore, they have the obligation for customer identification upon issuance.

Table 15 [Transition of Average Usage Amount of Electronic Money per Household a Month (Households of two and More Persons (2015–2017)]



Note: Data from the Ministry of Internal Affairs and Communications

Table 16 [Transition of the Ratio of households That Used Electronic Money Not Less Than 10,000 Yen a Month (Households of two and More Persons) (2015–2017)]



Note: Data from the Ministry of Internal Affairs and Communications

(2) Case

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

○ A case where electronic money obtained through fraud was sold via an internet broker and the paid money was remitted to an account opened in another person's name

and so on.

(3) Risk

Electronic money has a wide variety of forms and usages, but, in general, electronic money which falls under Prepaid Payment Instruments has excellent transportability and high anonymity. Actually, there are cases where electronic money is used in the process of money laundering.

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 charge value. In addition, under the present conditions, many issuers set the upper limit of charging and service places are limited to some specific member shops etc. On the other hand, in line with the spread of electronic money, there has been occurrence of cases of abuse of electronic money for crimes, including cases where victims required to pay usage fees related to fictitious paid sites purchased electronic money (prepaid cards) at convenience stores or other locations were deceived into revealing their ID and were defrauded of money equivalent in value to the face value of the prepaid cards (usage rights).

Therefore, relevant ministries and agencies and business groups are conducting initiatives to raise awareness about the risk from the viewpoint of preventing not only money laundering crimes but crime damage in general. In light of these circumstances, it is necessary to keep monitoring the usage of electronic money in Japan.

[Casino]

The Act on Maintenance of Specified Integrated Tourism Facilities and Areas (Act No. 80 of 2018) was enacted and it is necessary to take appropriate countermeasures for ML/TF, associated with casinos in the future. In a report published by FATF in 2009 and FATF recommendations, etc., the following is suggested:

According to a report published by FATF in 2009[*1], while casinos are lawfully operated outside Japan in several country and region, the risk of money laundering stems from the fact that

○ Casinos are businesses where cash is concentrated and they are often open 24 hours a day and a large amount of cash transactions happen quickly.
○ Casinos provide variety of financial services including accounts, exchange, remittance, and foreign currency exchange.
○ Some regions recognize casinos as places of amusement, not financial institutions, where countermeasures for ML/TF, are not taken sufficiently.
○ In some regions, the job separation rate of employees in the casino industry is high, and the education and training for countermeasures for ML/TF, are not provided sufficiently.

and so on are suggested.

And, in terms of the method of deception used in money laundering cases associated with casinos:
○ Purchasing chips using criminal proceeds and then exchanging them for cash without using them
○ Remittance of criminal proceeds from a casino account to other accounts using a casino chain
○ Purchasing chips of other guests with criminal proceeds
○ Exchanging a large amount of bills of small denominations or coins for bills of large denominations which are easier to control at a casino counter

and so on are suggested.

Relating to regulations on casinos, FATF's new "40 Recommendations" requests casino operators to take measures for customer control including the confirmation and checking of the identity of guests for financial transactions above 3,000 USD/Euros, to operate casinos under a license system as a measure to effectively implement countermeasures against money laundering and terrorist financing, to take legal measures in order not to make criminals or their related persons the owners or beneficiary owners of casinos or for other purposes, to have competent authorities supervise casinos effectively, among other matters.

Based on these requests, the Act on Maintenance of Specified Integrated Tourism Facilities and Areas, which was enacted this year, requires tp amend the Act on Prevention of Transfer of Criminal Proceeds to add casino operators to specified operators and to require casino operators to perform, for specified transactions including the delivery of chips, the verification of guests at the time of transaction, to prepare and retain transaction records, to report suspicious transactions, and so on. Furthermore, the Act on Maintenance of Specified Integrated Tourism Facilities and Areas stipulates implementing measures against money laundering by, in addition to the above-mentioned regulations, requiring the preparation and examination by the casino control committee of the regulations for prevention of transfer of criminal proceeds, requiring reports of exchange of cash and chips exceeding a specified amount to the casino control committee, regulations on the assignment and acceptance of assignment and taking out of chips and so on. The ACT makes it a goal to create an environment in which casinos are not misused for money laundering.

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

Section 4. High Risk Transactions

1. Transaction Type

By referring to cases in which foreigners visiting Japan were arrested for money laundering as well as situations that increase the risks of ML/TF ("non-face-to-face transactions" and "business that are cash-intensive") as described in the FATF's new "40 Recommendations" and its Interpretive Notes, we identified: (1) non-face-to-face transactions; (2) cash-intensive business; and (3) international transactions as the types of transactions that affect the risks of transactions. We then analyzed and assessed such transactions.

(1) Non-face-to-face Transactions

A. Factors that Increase Risks

(a) Characteristics

With the factors including development of Information Technology, 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, as well as customers can use mail order service which enables them to apply for the opening of bank accounts by mail. At financial instruments business operators, customers can conduct transactions such as opening of securities accounts or share trading through the Internet.

On the other hand, as business operators don't see their customers directly in non-face-to-face transactions, they cannot confirm customers' sex, age, appearance, behavior, etc. directly and judge whether the customers give false identification data or whether they pretend 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 false one or not. 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 deteriorate accuracy of customer identification.

Therefore, compared with face-to-face transactions, non-face-to-face transactions enable offenders to keep high anonymity, to falsify customer identification data such as name and address, and to 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 Evaluation, it was pointed out that customer identification and verification requirements for non-face-to-face transactions in Japan are insufficient.

(b) Case

The following are example cases of misuse of 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
- ○ Cases 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 destinations of remittance

and so on.

B. Measures to Mitigate Risks

The Act on Prevention of Transfer of Criminal Proceeds stipulates measures for customer identification that specified businesses operators need to take when customers' identification documents are not presented to them directly. These measures are: (i) Where specified business operators receive identification documents or copies thereof sent from customers, and send transaction

documents to the residence indicated in the identification documents or the copies thereof by registered mail with no forwarding address or the like; (ii) postal service providers visit the residence of customers on behalf of specified business operators, verify identification documents shown by the customers and inform specified business operators of customer identification data such as their name; and (iii) by electronic signature.

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 declare unoccupied address as their address by using copies of forged identification documents and receive 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 is planned to be implemented in April 2020.

The overview of the revision includes the following:

- ○ Regarding the identification documents to be sent to specified business operators in a customer identification measure where transaction documents are sent by mail requiring no forwarding, the businesses must receive one type of the original, etc., or otherwise, two types of copies 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 mail requiring no forwarding, the types of identification documents that may be presented by customers at the time of the 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 supporting FinTech and implemented on the day of promulgation.

The overview of the revision includes the following:

(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 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 requested the customers take using software provided by them, using records of customer identification 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 to introduce 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 for taking and sending images in (i) and (ii). Specified business operators are required to use appropriate software so that the accuracy of customer identification will not be negatively affected due to processing of the data being used. In addition, the identification documents usable for (i) and (ii) are limited to identification documents, etc. with photographs. Furthermore, other specified business operators stipulated in (ii) are limited to those who have a continuous transaction relationship with the customers and to deposit-taking financial institutions and credit card operators with necessary technology platforms that are maintained in relatively good condition.

These measures enable efficient customer identification to be completed online while maintaining a sufficient level of customer identification up to the present.

In addition, the Guidelines for Supervision by the Financial Services Agency provides that one of focal points of 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.

C. Assessment of Risks

As non-face-to-face transactions may hinder business operators from directly seeing customers and identification documents, accuracy of customer identification can be deteriorated. Therefore, compared with face-to-face transactions, non-face-to-face transactions facilitate offenders to keep high anonymity, to falsify customer identification data and to pretend to be a fictitious or another person by falsifying identification documents etc.

Actually, there are cases where non-face-to-face transactions were misused for money laundering, including a case where bank accounts opened by pretending to be another person were misused. Considering a relevant situation, it is recognized that non-face-to-face transactions have high risks to be misused for ML/TF.

(2) Cash Transactions

A. Factors that Increase Risks

(a) Characteristics

According to the statistics, in monthly average consumption expenditure of a household (2 or more persons) in 2014 by means of purchase, "cash" is 241,604 yen (82.5% in all consumption expenditure) and "credit card, monthly installment payment, and credit purchase (hereinafter referred to as "credit card etc.") is 46,995 yen (16.0% in all consumption expenditure). Although the transition of "cash" ratio shows decline as 93.5% in 2004, 88.8% in 2009 and 82.5% in 2014, purchase in cash is still the biggest part in consumption expenditure by means of purchase (see table 17). Use of cash in Japan is higher than that in other countries (see table 18).

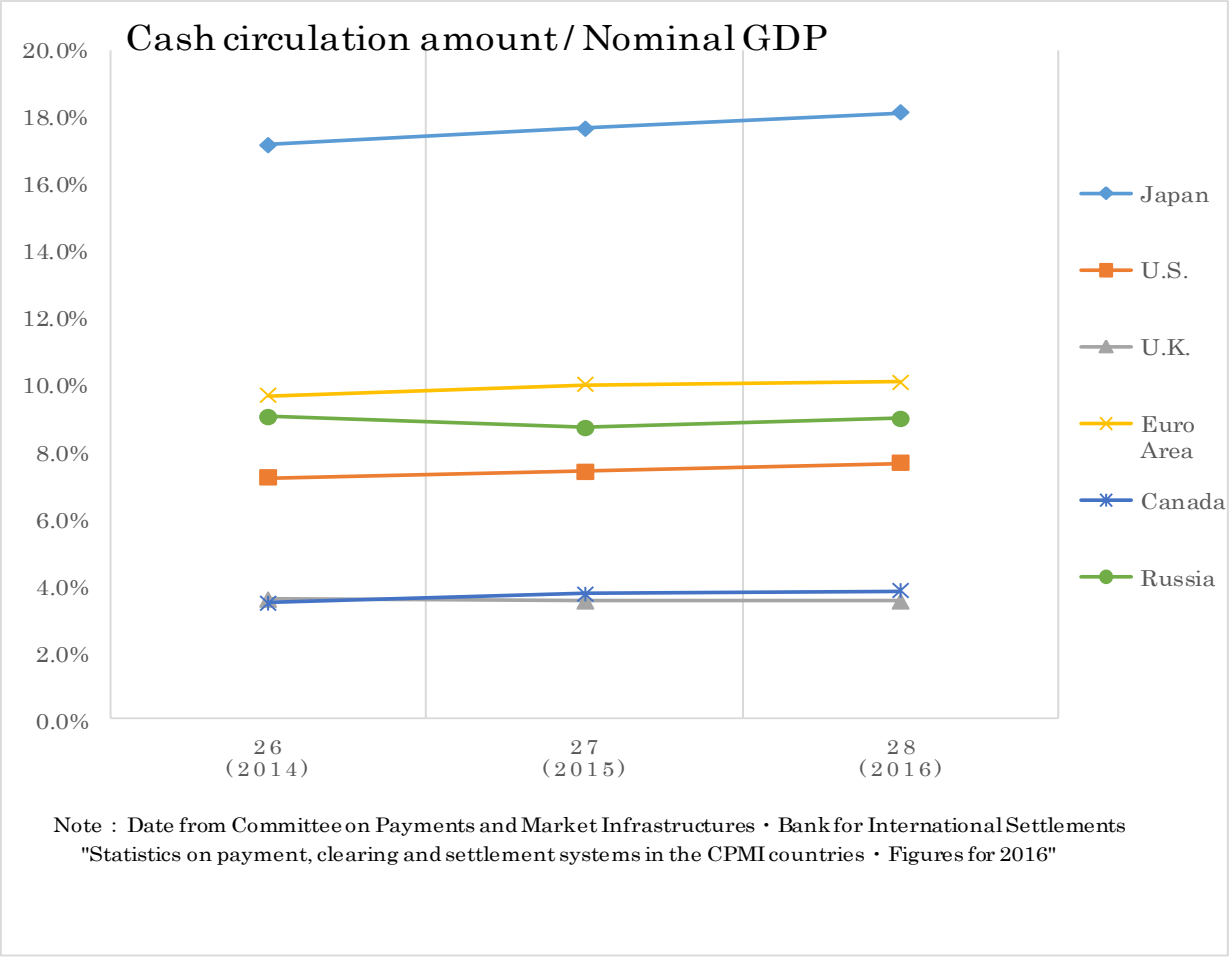
As to characteristics of cash transactions, they require certain amount of time to transfer physically, unlike exchange transactions which are a quick way to transfer funds to remote places. On the other hand, cash has high liquidity and transfer of ownership is easy. Along with that, cash transactions are highly anonymous unless they are recorded, and thus resulting in low visibility in tracing fund flow.

Table 17 [Expenditure by Type of Purchase (Two-or-more-person Households/ 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 of each country in nominal GDP (2014–2016)]



Note : Date from Committee on Payments and Market Infrastructures・Bank for International Settlements "Statistics on payment, clearing and settlement systems in the CPMI countries・Figures for 2016"

(b) Case

The following are example cases of misuse of cash transactions for money laundering:

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

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 two 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 supecified 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

In addition, the Secondhand Articles Dealer Act and the Pawnbroker Business Act require business operators to verify customer identification data such as address and name. This measure contributes to mitigate the risks of cash transactions.

Furthermore, competent administrative authorities provide supecified business operators with the "List of Reference Cases of Suspicious Transactions" etc. which indicate examples of potential suspicious transactions to which business operators should pay special attention. In the list, cases focusing on cash usage form are enumerated, such as

- ○ Transactions of large amounts of cash
- ○ Transactions that are made frequently in a short period and large in total, and business operators take them into account and take measures to file STRs properly

C. Assessment of Risks

In general, cash transactions have high liquidity and anonymity, and may hinder LEAs from tracing criminal proceeds. Especially, people are more likely to perform cash transactions in consumer expenditure in Japan. Therefore, cash transactions may hinder from tracing criminal proceeds unless business operators dealing with cash properly prepare transaction records.

Actually, there are many cases where money launderers misused cash transactions by, for example, pretending to be another person. Considering a relevant situation, it is recognized that cash transactions have high risks to be misused for ML/TF.

(3) International Transactions

A. Factors that Increase Risks

(a) Characteristics

In 2017, Japan's economy was the third largest in the world in terms of nominal GDP (approximately 546.6 trillion yen), the fifth largest in terms of the overall import value (approximately 75,379.2 billion yen, and the fourth largest in terms of overall export value (approximately 78,286.5 billion yen). Thus, Japan occupies an important position in the global economy. Japan also has a highly advanced financial market.

In the Japanese financial market, which is one of the leading international financial markets around the world, a huge amount of transactions is conducted. As indicated above, Japan is routinely conducting transactions with foreign countries. Compared with domestic transactions, international transactions, by their nature, may generally hinder LEAs from tracing funds because of the fact that national legal system and transaction system varies from country to country, and AML/CFT measures such as monitoring and supervision implemented in the home country may be unlikely applied in foreign countries.

Especially, in foreign exchange transactions, serial payment is frequently commissioned based on correspondent banking relationships and may be conducted in a short time through several intermediary banks at a distance. This may significantly hinder from tracing criminal proceeds.

In addition, in correspondent banking services, because financial institutions may not have direct relationships with remittance originators etc., they could be involved in money laundering unless respondent institutions develop internal control systems for AML/CFT. Furthermore, if a respondent institution is a fictitious bank that does not do business in fact (what is called "shell bank"), or if a respondent institution allows shell banks to use accounts, there is a high risk that foreign exchange transactions are used for ML/TF .

Some foreign countries and regions, in particular, accept systems that allow corporate directors and shareholders to be registered under the names of third parties. This situation is recognized to exist, where dummy corporations established in such countries and regions are misused to conceal criminal proceeds. In addition, passing through more than one such high-anonymity corporate account will increase the risk of the final transfer destination becoming unclear.

Recent years have also seen cross-border money laundering offences by international criminal organizations in which proceeds from fraud committed in foreign countries 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.

Furthermore, by disguising as foreign trade, purpose of remittance is easily justified and criminal proceeds could be transferred by paying more for the merchandise than it is truly worth.

Besides, in international transactions, cash courier (physical cross-border transportation of cash and other means of payment) may be misused for ML/TF, as well as the above-mentioned exchange transactions, etc. based on correspondent banking relationships.

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) Case

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

Analysis of the trends of arrests made in money laundering cases involving visiting foreigners reveals that Chinese, Vietnamese and Nigerians rank highly in terms of the number of arrested

foreigners by nationality. Recognized predicate offences include theft, fraud, and computer fraud. With respect to foreigners in Japan, "Section 2. Analysis of Money Laundering Cases, etc." of this report explains the results of the survey and analysis.

There have been cases in Japan of misuse of international 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.

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

○ 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 remittance destination of payment, deceived the company into remitting the payment to an account opened in the name of a shell company, and then withdrew a large amount of cash in one lump sum.

The main characteristics of these cases are that a large amount of money, sometimes over 100 million yen, is remitted each time, the reasons for remittance may be different between the receiver and the remitter, almost all the remitted amount may be requested to be paid out in cash, and remitters often request reverse transactions later.

There were cases of foreigners in Japan who operated unlicensed international remittance business, such as:

○ 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 into a foreign country in a travel bag

○ 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 to a foreign country in a deal disguised as a legitimate transaction and converted into cash there. This arrangement was in effect equivalent to an international remittance

and so on. The following are example cases abroad.

○ Cases 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.

Looking at the recent trend in international organized crime in Japan, we recognize that crimes are becoming increasingly sophisticated and difficult to detect because networks of criminals and crime-related locations are spread beyond a single country and criminals' roles are internationally divided. For example, organized-crime groups consisting of visiting foreigners in Japan commit crimes upon instruction from organized-crime groups located in their home countries. The resulting risk that proceeds derived from such cases may be recycled to other countries has been recognized.

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 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

*1 For example, the following obligations are imposed:
- Obligation to verify that the other party to correspondent banking relationships has an internal control system necessary to conduct verification at the time of transactions appropriately;
- Obligation to verify that the other party to correspondent banking relationships has not formed relationships for continuously

request to a respondent institution regarding a foreign exchange transaction involving remittance overseas, specified business operators must provide customer identification records of the originator to the institution; and - they must preserve customer identification records provided from a foreign exchange transaction operator whose country has similar legislation.

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

○ Proper examination and judgment of conclusion and continuation of correspondent banking relationships, including approval by supervisory compliance officers after collecting sufficient information of 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, as regards to cash couriers, when a person imports or exports by carrying means of payment, which is over 1 million yen for cash, checks, and securities, etc. or over 1 kg for precious metals, the person is obliged to submit written declaration to Finance Minister under the Foreign Exchange and Foreign Trade Act and to the Directors-General of Customs under the Customs Act.

The Ministry of Finance has improved the Foreign Exchange Inspection Manual, which indicates 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 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.

C. Assessment of Risks

Compared with domestic transactions, international transactions 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 was conducted through international transactions. Therefore, it is recognized that international transactions pose a risk for being misused in ML/TF.
In consideration of examples of situations that increase the risks of ML/TF as described in the FATF's new "40 Recommendations" and its Interpretive Notes as well as actual example cases, it is recognized that the following types of transactions have higher risks.

○ Transactions related to countries and regions where proper AML/CFT measures are not implemented

○ International remittance originated from a large amount of cash

---

or repeatedly performing exchange transactions with any financial institution etc. that does not have an internal control system necessary to conduct verification at the time of transactions appropriately; and

- the obligation to collect information on the AML/CFT systems developed by the other party to correspondent banking relationships, their business activities, and the status of supervision provided by administrative authorities of their country, and the obligation to clarify the responsibility of each party in conducting verification at the time of a transaction.

○ Transactions suspected that the customer provides false information about the purpose or source of funds of overseas remittance

2. Countries/Regions

We identified, analyzed, and assessed countries/regions that may affect the risks of transactions by referring to the situations that increase the risks of ML/TF listed in the Interpretive Note to the new "40 Recommendations" of FATF ("countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems") and the like.

(1) Factors that Increase Risks

FATF identifies jurisdictions (countries/regions) with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies; and issues public statements which call on its members to take AML/CFT measures in consideration of risks arising from the deficiencies.

Among others, in regard to North Korea, FATF has continuously called on its members and other jurisdictions to apply countermeasures to protect international financial system from the ongoing and substantial ML/TF risks emanating from the jurisdictions, since February 2011. The same request has been made continuously regarding Iran since February 2009. In June 2016, FATF evaluated the measures taken for Iran and suspended countermeasures for 12 months. In June 2017, FATF decided to continue the suspension of the 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, FATF public statement used to identify jurisdictions[*1] other than Iran and North Korea, and require members to take AML/CFT measures in consideration of risks arising from deficiencies associated with those jurisdictions, however, there is no such jurisdiction in the statement on October 19th, 2018.

(2) Measures to Mitigate Risks

Competent administrative authorities notified specified business operators of the FATF statement and asked them to thoroughly implement the duties of verification at the time of transaction and submission of STRs, as well as and 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 Guidelines for Supervision by the Financial Services Agency stipulates focal points for supervision which includes ample consideration of the manner of transactions (for example, payment amount, the number of times) with cross-checking the nationality (for example, a jurisdictions which are set out by FATF as not cooperative to implement AML/CFT standards) etc. and other relevant circumstances, in addition to taking account of the contents of this risk assessment report.

The Act on Prevention of Transfer of Criminal Proceeds and the Order stipulate that Iran and North Korea are jurisdictions where an AML/CFT system is deemed to be insufficient (hereinafter referred to as "specified jurisdictions"), and require that specified business operators shall, upon conducting a specified transaction with a person who resides or is located in the specified jurisdictions and any other specified transactions that involve transfer of property to a person who resides or is located in the specified jurisdictions, conduct enhanced verifying 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, it is recognized that transactions related to Iran or North Korea pose very high risks. In addition to the two jurisdictions, it is recognized that transactions related to countries to which appropriate attention should be paid in consideration of the statement have high risks, however, there is no such jurisdiction in the statement on October 19th, 2018. Even so, FATF published the names of countries/regions that have serious strategic deficiencies related to AML/CFT

---

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

measures and have developed action plans to deal with the deficiencies as countries/regions that continue to make improvement in compliance with international AML/CFT measures, and it is calling on those countries/regions to implement the action plans promptly within the proposed periods of time. Transactions which are conducted with those countries/regions before the deficiencies pointed out by FATF are resolved are recognized to have risks. Also, even if there are no direct transactions to these countries, malicious and shrewd methods may be used to redirect funds through neighboring countries/regions. Therefore, 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 (2016 to 2018) regarding the designation of countries/regions targeted for FATF's monitoring process to improve observance of FATF statements and AML/CFT measures. Note that the countries/regions announced during FATF's general meeting in October 2018 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 FATF called on its members and other jurisdictions to apply countermeasures]

Legend: ● indicates that FATF requested its members and other jurisdictions to apply countermeasures; ◎ indicates that FATF asked its members and other jurisdictions to conduct strict customer management

Countries/regions and time	2016			2017			2018		
	Feb	Jun	Oct	Feb	Jun	Nov	Feb	Jun	Oct
Iran	●	◎	◎	◎	◎	◎	◎	◎	◎
North Korea	●	●	●	●	●	●	●	●	●

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

Legend: ○ indicates that FATF designated it as a monitoring process to improve observance of AML/CFT measures]

Countries/regions and time	2016			2017			2018		
	Feb	Jun	Oct	Feb	Jun	Nov	Feb	Jun	Oct
The Bahamas									○
Botswana									○
Ethiopia				○	○	○	○	○	○
Ghana									○
Pakistan								○	○
Serbia							○	○	○
Sri Lank						○	○	○	○
Syria	○	○	○	○	○	○	○	○	○
Trinidad and Tobago						○	○	○	○
Tunisia						○	○	○	○
Yemen	○	○	○	○	○	○	○	○	○
Afghanistan	○	○	○	○					
Bosnia and Herzegovina	○	○	○	○	○	○			
Guyana	○	○							
Iraq	○	○	○	○	○	○	○		
Laos	○	○	○	○					
Myanmar	○								
Papua New Guinea	○								
Uganda	○	○	○	○	○				
Vanuatu	○	○	○	○	○	○	○		

3. Customer Type

We identified, analyzed, and assessed the customer types that affect the risks of transactions by referring to cases in which members of organized crime groups were arrested for money laundering and severe terrorism issues; situations that increase the risks of ML/TF listed in the Interpretive Note to the new "40 Recommendations" of FATF ("non-resident customers" and "the ownership structure of the company appears unusual or excessively complex"); the matters pointed out in the Third Round Mutual Evaluation of Japan by 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 organized crime groups) 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 with unclear beneficial ownership.

(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 fund raising activities by disguising them as or misusing business operations.

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

There exist Boryokudan throughout Japan. Their size and activity vary. As of October 1, 2018, 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 2017, the total number of Boryokudan gangsters is 34,500,[*2] including 16,800 Boryokudan members and 17,700 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 theft, Boryokudan commit various crimes to obtain funds according to changes in the times, such as bank-transfer scams and other specialized fraud and smuggling of gold bullion. Also these days, Boryokudan are more careful about concealing their organizations' actual condition. Since they disguise their activities as business operations or claim to be political activists or social campaigners and the like, it is becoming increasingly difficult to define them. Furthermore, they often commit money laundering and make relationships between each fund raising activity and its result unclear, in order to avoid taxation on or confiscation of gained funds or being arrested due to the gained funds. Criminal proceeds are funds to maintain and strengthen organizations by using them as "operating capital" for further crimes or expenses to obtain weapons, etc. The criminal proceeds are also used for going into legal businesses.

Also in recent years, quasi-Boryokudan conducting violent illegal behavior, etc. such as gang-bashing, inveterate violence in shopping streets and amusement areas has been observed. There are some quasi-Boryokudan who are not clearly organized to the same level as Boryokudan, but seem to have a close relationship with crime syndicates such as Boryokudan. It appears that they are adept at obtaining funds efficiently or on a large-scale through various crimes designed to raise funds and certain business activities.

---

*1 They are groups/individuals that pursue economic profits through the use of violence, threats and fraudulent method, and 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.

With respect to Boryokudan, the item "Boryokudan" in "Section 2. Analysis of Money Laundering Cases, etc." of this report explains the results of surveys and analysis.

(b) STRs

There were 1,200,642 STRs from 2015 to 2017, including 194,805 reports (or 16.2% of total reports) related to Boryokudan gangsters.

(c) Case

There were 1,138 cases cleared of money laundering from 2015 to 2017, including 220 cases (19.3% of total cases) related to Boryokudan gangsters.

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

- ○ Cases 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.
- ○ Cases where Boryokudan received criminal proceeds in the name of protection fees, contributions, etc., by taking advantage of their organizations' threatening behavior
- ○ Cases where Boryokudan members received criminal proceeds by making criminal proceeds from prostitution transferred to the account in thename of his/her relative knowingly

.

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 on Measures Against Crimes) has been formulated to help companies, including deposit-taking institutions, to cut any relationships with anti-social forces.

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

And financial institutions etc. are introducing clauses to exclude Boryokudan etc. into their terms and conditions of transactions. This is the efforts to dissolve business relationships in case a customer has turned out to be Boryokudan etc. Furthermore, as general business practices, if a customer has turned out to be a member of anti-social forces, financial institutions etc. shall consider making STRs under the Act on Prevention of Transfer of Criminal Proceeds.

C. Assessment of Risks

Other than committing various crimes to gain profit, Boryokudan and other anti-social forces conduct fund raising activities by disguising them as or misusing business operations. As money laundering makes the source of funds from criminal activities or fund raising activities unclear, money laundering is indispensable for anti-social forces. Considering a relevant situation, it is recognized that transactions with anti-social forces have high risks of ML/TF.

(2) International Terrorists (Such as Islamic Extremists)

The current terrorism issues remain very severe with many terrorist attacks occurring in Europe and the U.S. Also, there is a concern that foreign fighters who participated in battles in Iraq and Syria may commit terrorism after returning to their 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. Matters concerning terrorist financing have increased and become more complicated.

In this assessment report, we have referred to the new "40 Recommendations" of FATF, its Interpretive Notes, FATF's reports, and measures under the Act on Prevention of Transfer of Criminal Proceeds to take account of the following comprehensively:

○ Threats (terrorist groups such as ISIL[*1], AQ[*2] and other Islamic extremists and their financiers)
○ Vulnerabilities (legal and illegal sources and methods of terrorist financing)
○ 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) Characteristics

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. In 2017, however, ISIL lost most of its territory in Iraq and Syria due to attacks from the military of these countries with the support of other nations.

However, ISIL continue to conduct terrorist attacks in European and American countries that participate in the anti-ISIL coalition. During such an attack, ISIL called for fighters to use knives, vehicles, etc. when bombs or firearms are unavailable, and as a result several terrorist attacks occurred in European and American countries during 2017. Also, in May of the same year, a force supporting ISIL occupied part of Marawi, a city in the southern part of the Philippines. The battle between that force and the Philippine government continued for five months.

It seems that the number of foreign fighters participating in ISIL has decreased due to the fact that ISIL lost most of its territory in Iraq and Syria and that countries took measures to prevent foreign fighters from entering Iraq and Syria. However, there is a concern that foreign fighters who participated in battles in Iraq and Syria may commit terrorism after returning to their countries or moving to a third country in the future, and that many foreign fighters flowing into conflict areas other than Iraq and Syria may intensify or prolong the conflicts in such areas or may spread their extreme ideology across the world.

As for AQ and its related organizations, Ayman al-Zawahiri, a leader, has been repeatedly asserting the idea of anti-Americanism and anti-Israelism. Meanwhile, Hamza bin Laden, a son of Osama bin Laden (the leader when AQ was organized), is calling for fighters to practice terrorism against the US, etc. through the Internet. Also, as AQ-related organizations operating in the Middle East, Africa, and South Asia regions have been committing terrorism targeted at government organizations and the like, and calling for fighters to practice terrorism in European and American countries through online newsletters, etc., AQ and its related organizations are still a great threat. The United Nations Security Council has adopted resolutions (No. 1267 and succeeding

---

*1 Acronym of the Islamic State of Iraq and the Levant. Although ISIL used to be a group affiliated with Al-Qaeda, it separated from Al-Qaeda 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 of Al-Qaeda.

resolutions as well as No. 1373) to freeze the assets of or implement measures against persons who are related to AQ or other terrorist groups. However, 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 so far.

However, 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 suspect that there are people from Japan who have made attempts to travel to Syria in order to join ISIL as fighters.

In light of the matters to related to the threat of and vulnerability to terrorist financing that have been internationally pointed out, 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.

FATF also has requested 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 organization.

The FATF Recommendations highlight forms of misusing nonprofit organizations: a terrorist organization pretends to be a legitimate group; a legitimate group is used as a pipeline for terrorist financing; funds 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 a considerable fund sources, 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 another party responsible for disbursing funds for their activity 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

*1 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."

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 relationship with a terrorist organization overseas.

Note that the establishment and management of nonprofit organizations in Japan are regulated by the Act to Promote 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 international remarks on the transfer of terrorist funds by misused nonprofit organizations when engaging in financial transactions, etc. in light of the position, roles, etc. of Japan as an international financial market.

(b) STRs and Case

Although nobody has been arrested in Japan in relation to terrorist financing, the following case has been recognized:

○ In one fraud case, a corporate executive was arrested 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 is deemed to have been supporting the Japanese Red Army members on the international wanted list, and almost all of the deposited money was withdrawn in a foreign country.

The Japanese Red Army has caused numerous international terrorism incidents in the past. Seven members still remaining at large are on the international wanted list, and initiatives continue in efforts to arrest fugitive members and reveal the organization's activities.

STRs suspected of being related to terrorist financing have been filed by specified business operators. Some were reported after a transaction was found to be made with the same name as an individual who is subject to asset freezing and other measures, or an individual who has been linked with terrorist groups, while others were reported after business operators looked at the customer type, transaction form, 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.

Compared with money laundering, terrorist financing has the following characteristics:

○ Terrorist financing is not necessarily obtained through illegal means
○ The value of transactions related to terrorist financing may be small
○ Terrorist financing tends to be provided not only directly to regions under terrorist groups' control, but also via the neighboring countries

Therefore, it is critical to keep in mind the following matters in addition to focusing on money laundering when filing STRs related to terrorist financing.

○ Customer attributes
Customer identification data, including the names, aliases and birthdates, concerning persons subject to asset freezing under the Foreign Exchange and Foreign Trade Act and the Act on Special Measures concerning International Terrorist Assets Freezing.

○ Countries/regions
Whether remittance destinations and sources are countries/regions where terrorist groups are conducting activity (Iraq, Syria, Libya, Nigeria, Yemen, Afghanistan, Pakistan, Somalia, Lebanon, etc.) or countries/regions in their neighborhood.

○ Transaction form
- 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.

B. Measures to Mitigate Risks

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 the 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 be reported as an STR under the Act on Prevention of Transfer of Criminal Proceeds. In addition, in light of the risk of virtual currency being misused for terrorist financing that has been internationally pointed out, the revised Act on Prevention of Transfer of Criminal Proceeds, under which virtual currency exchange service providers have been added as specified business operators, was put into force 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 entered into force for Japan on August 10 of the same year.

In addition, the National Police Agency requires specified business operators to always perform their obligation of verifying transactions at the time of transfer in accordance with the Act on Prevention of Transfer of Criminal Proceeds and file STRs through competent administrative authorities each time the list of groups subject to asset freezing and other countermeasures, adopted as United Nations Security Council resolutions (No. 1267 and its succeeding resolutions and No. 1373), is updated.

○ 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 meet the global request for the implementation of 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 for Threatening the General Public" (Article 1) and sets forth punishments for the provision of funds or other benefits to carry out Criminal Acts for Threatening the General Public (Articles 2 to 5).

In addition to the provision of funds, the provision of land, buildings, properties, services and other benefits to supporters who attempt to provide funds, etc., to terrorists who plan to commit Criminal Acts for Threatening the General Public are subject to punishment under the Act.

○ Foreign Exchange and Foreign Trade Act

With respect to international transactions, in response to the United Nations Security Council resolutions (No. 1267 and its succeeding resolutions and No. 1373) of asset freezing and other measures, simultaneous asset freezing by G7 and various asset freezing measures have been implemented against individuals and groups subject to such measures in accordance with the Foreign Exchange and Foreign Trade Act. More specifically, as of November 2, 2018, 406 individuals and 106 groups have been designated as such individuals and groups.

○ Act on Special Measures concerning International Terrorist Assets Freezing

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 such measures under the Act on Special Measures concerning International Terrorist Assets Freezing, which came into effect in October 2015. More specifically, as of November 2, 2018, the names of 406 individuals and 106 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 held by them and retain it. Order for Enforcement of the Terrorist Assets-Freezing Act was amended to add virtual currency into the regulated assets, and the revision took effect in April 2017.

C. Assessment of Risks

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 internationally pointed out, there are risks that the following activities may be conducted in Japan:

- ○ Members of Islamic extremist and other terrorist groups hide themselves in communities of people from Islamic countries and misuse the communities for fund raising.
- ○ Foreign fighters engage in fund raising and other activities.
- ○ Terrorist financing may be provided through transactions disguised as legitimate ones conducted by Japanese organizations and companies.

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 is a highly secretive activity and most of the terrorism-related information collected is fractional, it continues to be necessary to accumulate further information and conduct a continuous and comprehensive analysis in light of the abovementioned risks.

(3) Non-resident Customers

A. Factors that Increase Risks

Non-residents who trade through mail, Internet, etc. while staying in a foreign country (hereinafter referred to as "non-resident customers") always make non-face-to-face transactions so they can keep high anonymity. Therefore, it is easy for them to falsify customer identification data or to pretend to be a fictitious or another person by altering their customer identification documents. In addition, in ongoing business relationships with non-resident customers, when they are suspected of falsifying identification data that has already been verified or when their bank accounts are suspected of being misused for ML/TF, business operators may have fewer measures to conduct appropriate CDD, such as verifying customer identification data, compared with customers residing in Japan.

In the Interpretative Note of New "40 Recommendations," FATF states that "Non-resident customers" is one of the potentially higher-risk situations.

B. Measures to Mitigate Risks

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

C. Assessment of Risks

Transactions with non-resident customers are conducted through non-face-to-face transactions. Because of that, they can keep high anonymity and it is easy for them to falsify customer identification data or to pretend to be a fictitious or another person. At the same time, business operators have limited measures to conduct ongoing CDD, compared with customers residing in Japan. Considering a relevant situation, it is recognized that transactions with non-resident customers have high risks of ML/TF.

(4) Foreign Politically Exposed Persons

A. Factors that Increase Risks

Foreign PEPs (Heads of State, senior politicians, senior government, judicial or military officials, etc. are shown as examples by FATF) have positions and influences 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, strictness of laws to cope with corruption varies from jurisdiction to jurisdiction.

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, FATF established guidelines about PEPs and expressed its opinion that PEPs have potential risks to commit ML/TF or predicate offenses, including embezzlement of public funds and bribery, because of their position, so operators should 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 phenomenon which influence on any society and economy. Countries have come to share the recognition that comprehensive approach, including international cooperation, is necessary to promote efficient corruption prevention measures. Measures to prevent transfer of proceeds derived from corruption by foreign public officials are required internationally. In this circumstance, 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 are some cases of violation of the Unfair Competition Prevention Act in recent years, including a case where a worker of an overseas subsidiary of a Japanese company gave a set of golf clubs to a foreign government official as bribery, a case where a worker of a Japanese company handed cash to a foreign public official in reward for the road construction work in a project of Official Development Assistance (ODA) in a foreign country, a case where a worker of an overseas subsidiary of a Japanese company handed cash etc. to an official of local customs in reward for overlooking illegal operation of the company and a case where an employee of a Japanese company handed cash to a foreign public official in reward for concluding an advantageous contract of consultation service for a railroad construction in an ODA project in a foreign country.

B. Measures to Mitigate Risks

When specified business operators conduct specified transactions with (1) the Head of a foreign 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 and its Order and Ordinance require that the business operators shall conduct enhanced CDD, including verifying the source of wealth and source of funds as well as customer identification data etc.

In addition, the Guidelines for Supervision by the Financial Services Agency stipulates that one of the focal points of supervision 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 Order and Ordinance.

C. Assessment of Risks

Foreign PEPs have the positions and influences that can be misused for ML/TF. Grasp of their identification data etc. is limited, and efforts to introduce anti-corruption measures varies from

jurisdiction to jurisdiction. Depending on the situation, we recognize that transactions with foreign PEPs carry high risks of ML/TF.

(5) Legal Persons without Transparency of Beneficial Ownership

A. Factors that Increase Risks

(a) Characteristics

Legal persons in Japan include stock companies, general partnership companies, limited partnership companies, and limited liability companies, and all of these legal persons conducting corporate activities obtain legal personality by registering the entity according to the Commercial Registration Act.

As stock companies and other legal persons can be independent owners of property, a natural person can change his/her ownership of property without any 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.

For examples, various people, including shareholders, directors, executive officers, and even creditors, have different rights for the company's property. Hence, if property is transferred to a legal person, the natural person who has the beneficial ownership of the property can be easily concealed owing to the complex right/control structures peculiar to legal persons.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 structures 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. placement of a third party, who is under their control, as a director of the legal person).

Cases of arrest in relation to 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 ownership is unclear. The following are examples 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.Among money-laundering offences leading to arrests from 2015 to 2017, such modus operandi were used in 21 cases. In terms of the form of misused legal persons, stock companies accounted for the majority, followed by limited liability companies and special limited liability companies[*1] in several cases each.

The background to many cases of misusing stock companies is that organized crime groups take advantage of the social recognition and high credibility of stock companies, which are used for

---

*1 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 in the former act,“limited liability company (yugen gaisya)” is no longer available. Limited liability companies(yugen gaisya) existing as of the enforcement date of the Acts continue to exist as stock companies (such companies are referred to as "special limited liability companies"). There are special provisions in the Companies Act, such as that the name of a special limited liability company shall include the term "limited liability company(yugen gaisya)."

solicitation of investments and for transactions involving transfer of a large amount of funds.

In terms of predicate offenses, 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 are misused for professionally and systematically committed crimes that generate a large amount of proceeds.

Moreover, it is said that in so-called offshore financial centers, which refers 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. 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,

FATF requires that 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.
- ○ To have mechanisms where beneficial ownership of legal persons can be identified, as well as to ensure that competent authorities can obtain or access information on beneficial ownership of legal persons in a timely manner.
- ○ Considers measures to simplify business operators' access to beneficial ownership and control information.

Other than that, in Japan, there are business operators who provide legal persons etc. with an address, facilities, communication means for business/management sake as follows.

- ○ Postal receiving service providers
  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 them to the customer.
- ○ Telephone receiving service providers
  They authorize a customer to use their telephone number as the customer's contact telephone number, then receive telephone calls addressed to the customer, and transmit the content to the customer.
- ○ Telephone forwarding service providers
  They authorize a customer to use their telephone number as the customer's contact telephone number, then automatically forward telephone calls addressed to or received from the customer to the telephone number designated by the customer.

By misusing services of these providers, it is possible to establish and maintain a legal person that has no physical presence, to be specific, by providing others with an address or a telephone number which actually aren't used by the legal person and making up fictitious or exaggerated appearances of business reliability, business scale, etc.

(b) Case

The following are example cases of misuse of legal persons for money laundering:

- ○ A case where a beneficial owner of a company, who established it while placing a third party as a representative director, concealed proceeds from fraud in the company's bank account.
- ○ 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 internet sales of electronic books and applicants for the side businesses were defrauded of money as they were made to remit money in the name

of expenditures necessary for a server upgrade.

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

and so on.

B. Measures to Mitigate Risks

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 identification of a customer's beneficial owner if the customer is a legal person.

In addition, the Guidelines for Supervision by the Financial Services Agency stipulates that one of the focal points of supervision is whether a system necessary to conduct verification appropriately at the time of transactions, such as verification of the beneficial owner when conducting transactions with a legal person, has been established.

Also, the Companies Act stipulates the deemed dissolution of dormant companies[*1]. This is a system intended to mitigate the risk of legal persons obtaining dormant companies through resale or illegal registration changes, etc. and misusing them for crimes. Over 20,000 cases of deemed dissolution have been occurring every year since FY2014, with approximately 87,000 cases in FY2014, 21,000 cases in FY2015, and 21,000 cases in FY2016.

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 above-mentioned 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 make service contracts. The Act also requires service providers 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, through taking account of the contents of this risk assessment report, and a comparison with the manner of ordinary transactions and the like, in addition to the result of verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

C. Assessment of Risks

By placing property in the complex right/control structures of legal persons, a natural person who has substancial ownership of the property can be easily concealed. Because of such characteristics of legal persons, it becomes difficult to track funds owned by legal persons without transparency of beneficial ownership.

Actually, there are, for example, cases where a bank account, which was opened in the name of a legal person without transparency of beneficial ownership, was misused to conceal criminal proceeds derived from fraud and other crimes. Considering a relevant situation, it is recognized that transactions with legal persons without transparency of beneficial ownership have high risks of ML/TF.

---

*1 A stock company for which 12 years have elapsed from the day when a registration regarding such stock company was last effected.

[Customers Who Use an Identification Document without a Photograph]

○ Risks specific to identification documents without a photograph

Concerning 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 case of photographic ID, business operators can compare the photo on the ID and the appearance of the customer in front of them and can confirm their identity.

On the other hand, the reliability of identification by non-photographic ID is lower than that by photographic ID although non-photographic ID is also issued only to the person to be verified and it helps identification between the person to be verified and the person who brings it.

If non-photographic ID is used for customer identification documents, business operators might not be able to detect a person who pretends to be another when conducting verification at the time of a transaction. 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 FATF, it is 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 FATF, revision of the Act on Prevention of Transfer of Criminal Proceeds of 2014 and the accompanying revision of the order for enforcement of this act and the relevant ordinance specify the following measures as the methods for identifying specific persons when customers submit non-photographic ID: (i) not unnecessarily sending documents related to the transactions to the residence written on the relevant identification document by registered mail, (ii) 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 (iii)), and (iii) requiring other identification documents or a copy thereof, or supplementary documents or a copy 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 differences in risks between the customer identification method using photograph ID and the customer identification method using non-photographic ID have become small. 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 of Money Laundering and Terrorist Financing reports assessed that transactions with customers presenting non-photographic ID have higher risks than transactions using photographic ID, it is recognized that the risks have been lowered.

On the other hand, given that reliability of identification by non-photographic ID is still lower than that by photographic ID, it is necessary to follow the customer identification method based on the Act on Prevention of Transfer of Criminal Proceeds and to continue to focus on cases where customers deliberately refuse to present photographic ID as cases that present a risk of misuse for ML/TF.

Section 5. Low Risk Transactions

1. Factors to 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 to be misused for ML/TF.

(i) Transactions that have a clear source of funds

When characteristics or ownership of a source of funds is clear, it is difficult to misuse 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 source/destination 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 that provide legal persons etc. with an address, facilities, means of communication for business/management have 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 regulation threshold are inefficient for ML/TF. In the Recommendations and Interpretative Notes etc., FATF also sets out transaction amounts which are the threshold 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 high risks of 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 person who, in conformity of business regulations, obtained a business license from the State etc. Customers' identity is clear and fund traceability is secured in such transactions.

---

*1 The Act on Prevention of Transfer of Criminal Proceeds and its 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 single transaction divided, the transactions should be regarded as a single transaction.

2. Low Risk Transactions

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

These transactions are prescribed by the current Ordinance as those permitting simplified CDD measures, 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 to manage the customer, it is not recognized as a low-risk transaction. [*1]

(1) Specified Transactions in Money Trusts, etc. (Article 4, paragraph 1, item 1 of 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 falls under the transactions with factors to mitigate risks;(i), (iii), (iv) and (viii). Therefore, they are deemed to be low-risk.

(2) Conclusion etc. of Insurance Contracts (Article 4, paragraph 1, item 2 of Ordinance)
Conclusion etc. of insurance contracts including each transaction prescribed in Article 4, paragraph 1, item 2 of Ordinance (A: Insurance contracts without payment of maturity insurance money etc., B: Insurance contracts that total repayment is under 80% of total premium) fall under the transactions with factors to mitigate risks; (vi). Therefore, they are deemed to have low risks.

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

A. Payment of Maturity Insurance Claims etc. for Insurance Contracts whose Total Repayment is less than the Total Premium
Payment of maturity insurance money etc. of insurance contracts that total repayment is under 80% of total premium, prescribed in Article 4, paragraph 1, item 3, (a) of Ordinance fall under the transactions with factors to mitigate risks;(vi). Therefore, they are deemed to have low risks.

B. Payment of Maturity Insurance Claims etc. for Qualified Retirement Pension Contracts, Group Insurance Contracts, etc.
Payments for maturity 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 be low-risk.

(4) Transactions Carried out on a Securities Market etc. (Article 4, paragraph 1, item 4 of Ordinance)
Buying and selling of securities carried out on a securities market etc.,[*3] as prescribed in Article 4, paragraph 1, item 4 of the Ordinance fall under the transactions with factors to mitigate risks; (iii) and (viii). Therefore, they are deemed to be 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 Ordinance)
That Are Settled by an Account Transfer at the Bank of Japan (Article 4, paragraph 1, item 5 of 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 Ordinance fall under the transactions with factors to mitigate risks; (iii) and (viii). Therefore, they are deemed to have low risks.

(6) Specified Transactions Concerning Loan of Money etc. (Article 4, paragraph 1, item 6 of 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

---

*1 In the Act on Prevention of Transfer of Criminal Proceeds and its enforcement order, any transaction that permits simple customer control provided for by the rule is excluded from specific transactions that require verification when carrying out the transaction. However, this does not exclude specific tasks related to preparing and keeping transaction records and reporting suspicious transactions -- they are subject to prescribed customer controls. In addition, the law stipulates that if the transaction is suspicious or is one that requires special attention in managing the customer, then such transaction is a target for verification when carrying it out in addition to other specific transactions, even if the transaction would normally qualify for simple control.

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

*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.

Article 4, paragraph 1, item 6, (a) of the Ordinance fall under the transactions with factors to mitigate risks; (iii) and (viii). Therefore, they are deemed to be low-risk.

B. Loans etc. Based on Insurance Contracts etc. that Total Repayment Is Less Than the Total Premium

Loans etc. based on insurance contracts etc. of 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 the transactions with factors to mitigate risks;(i), (iii), (iv) and (vi). Therefore, they are deemed to be 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 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 exceed 2 million yen is provided as a mortgage, prescribed in Article 4, paragraph 1, item 7, (a) of Ordinance fall under the transactions with factors to mitigate risks; (i) and (viii). Therefore, they are deemed to have low risks.

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 Ordinance fall under the transactions with factors to mitigate risks; (viii). Therefore, they are deemed to have low risks.

C. Payment of Utility Charges

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

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 the transactions with factors to mitigate risks; (viii). Therefore, they are deemed to be 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 the transaction with factors to mitigate risks; (vii) and (viii). Therefore, they are deemed to be 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 which 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 Ordinance fall under the transactions with factors to mitigate risks; (vii) and (viii). Therefore, they are deemed to have low risks.

(8) Opening a Special Account under the Act on Transfer of Bonds, Shares, etc. (Article 4, paragraph 1, item 8 of Ordinance)

Opening a so-called special account [*2]under the Act on Transfer of Bonds, Shares, etc., prescribed in

---

*1 Individual credit is a transaction form. When purchasers buy products from sellers, purchases don't use 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, tie-up loan is a kind of individual credit. There are tie-up loans that financial institutions and sellers cooperate to provide funds for sales contracts or service provision contract and tie-up loans that purchasers apply to individual credit operators, 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 which is opened in a trust bank by a company issuing shares when the company doesn't know the account of

Article 4, paragraph 1, item 8 of Ordinance, falls under the transactions with factors to mitigate risks; (iii) and (viii). Therefore, it is deemed to have low risks.

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

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

(12) Specified Transactions in Telephone Receiving Service Contracts (Article 4, paragraph 1, item 12 of Ordinance)

Specified transactions in telephone receiving service including transactions prescribed in Article 4, paragraph 1, item 12 of Ordinance (A: a service contract of telephone receiving service in which indicating that being a telephone receiving service provider to a third party is included, B: contract of call center business etc.[*2]) fall under the transactions with factors to mitigate risks; (v). Therefore, they are deemed to have low risks.

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

A. Transactions That the State etc. Conduct 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 Ordinance fall under the transactions with factors to mitigate risks; (i), (ii), (iii), (iv) and (viii). Therefore, they are deemed to have low risks.

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 Ordinance fall under the transactions with factors to mitigate risks; (i), (iii), (iv) and (viii). Therefore, they are deemed to have low risks.

(14) Specified Transactions in Agent Work etc. for Specified Mandated Acts by a Judicial

---

shareholders.

*1 Transactions which are 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) is designated by the matter of designating communications method (Public Notice of the Financial Services Agency No. 11 of 2008) prescribed in Article 4, paragraph 1, item 9 of Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds

*2 Businesses conducted by taking telephone calls (including telecommunications by facsimile devices) for receiving applications for contracts to provide explanations about or consultation on goods, rights, or services or to provide the goods, rights or services or for concluding such contracts. Concrete examples of call center business include counter for material request and inquiry, customer center, help desk, support center, consumer inquiry counter, maintenance center, and order reception center.

Scrivener etc.[*1] (Article 4, paragraph 3 of Ordinance)

A. Conclusion of a Voluntary Guardianship Contract

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

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

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

*1 As to 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 two million yen or less are excepted.