Tentative Translation

November 2017

National Risk Assessment of Money Laundering and Terrorist Financing

National Public Safety Commission

Abbreviations for Laws

Abbreviations for laws are as follows.

[Abbreviation]	[Law]
Foreign Exchange and Foreign Trade Act	Foreign Exchange and Foreign Trade Act (Act No. 228 of 1949)
Act on International Terrorist Assets-Freezing	Act on Special Measures Concerning International Terrorist Assets-Freezing, etc. Conducted by the Government 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)
Interest Deposit and Interest Rate 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 Financing of Offences of Public Intimidation	Act on Punishment of the Financing of Criminal Activities for the Purpose of Intimidation of the General Public and of Governments (Act No. 67 of 2002)
Act on Prevention of Transfer of Criminal Proceeds	Act on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007)
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 Law	Act concerning Special Provisions for the Narcotics and Psychotropics Control Act 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. Purpose 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/or terrorist financing (hereinafter referred to as "ML/TF") is always changing. Global countermeasures under the cooperation of countries are required in order to strongly cope with the problem.

FATF (Financial Action Task Force) *2 requests countries to identify national ML/TF risks and assess them in compliance with the new "40 Recommendations", which were revised in February 2012. *3

In addition, in G8 Lough Erne Summit held in June 2013, considering the present state that companies etc. with nontransparent ownership/control structure are misused for money laundering and tax avoidance, G8 Action Plan Principles were agreed, which include, among others, 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, based on the FATF's new "40 Recommendations" and G8 Action Plan Principles, Japan set up a working group consisting of the National Police Agency and other relevant ministries and agencies including the Financial Services Agency in order to assess ML/TF risks in transactions. In December 2014, the National Police Agency published "National Risk Assessment of Money Laundering and Terrorist Financing".

2. Purpose

The Act on Prevention of Transfer of Criminal Proceeds was amended in 2014. Based on the newly provided Article 3, paragraph 3 of the Act[*4] and relevant materials including above-mentioned national risk assessment 2014, this new national risk assessment report has been made and it indicates risks etc. in each category of transactions carried out by business operators.*5

Given that FATF Recommendation 1 calls on countries to "identify and assess the ML/TF risks for the country" and that the Interpretive Notes to the FATF Recommendation 1 require business operators to "take appropriate steps to identify and assess ML/TF risks for" their products and services or implement a risk based approach, Japan implemented the revised Act on Prevention of Transfer of Criminal Proceeds and the Order and Ordinance for Enforcement of the revised Act on October 1, 2016, urging specified business

---

∗1 In general, money laundering means an act to conceal the source or real owners of criminal proceeds so that the offenders could prevent investigating authorities from finding the proceeds or arresting them. In Japan, the Act on Punishment of Organized Crimes and the Anti-Drug Special Provisions Law prescribe money laundering offenses.

∗2 Abbreviation of "The Financial Action Task Force". It is an intergovernmental body to promote international cooperation regarding AML/CFT measures.

∗3 FATF set out measures which countries should take in law enforcement, criminal justice and financial regulation area in order to fight against ML/TF, as FATF Recommendations.

*4 Article 3, paragraph 3 of the Act provides as follows: "The National Public Safety Commission is to, each year, conduct investigation and analysis on the status of the transfer of criminal proceeds including the modes employed for the transfer of criminal proceeds, and, for each category of transactions carried out by business operators including specified business operators, prepare and publish a report of national risk assessment of money laundering and terrorist financing which includes the results of the investigation and analysis including the risk of transfer of criminal proceeds by way of these transactions.

∗5 Money laundering and terrorist financing differ in the following points: (i) while money laundering involves criminal proceeds obtained by illegal means, 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 and regions which require caution when sending funds are different between money laundering and terrorist financing. This report describes the risk of terrorist financing based on these differences. However, because terrorist financing itself is a crime and the funds themselves could be treated as criminal proceeds under money laundering regulations, it is thought that those who plan to terrorist financing attempt to conceal their transfer of funds, like other criminal proceeds, by misusing various transactions, products and services. Thus, the risks in transactions and products/services referred to in this national risk assessment include terrorist financing risks.

operators to take measures to make determination as to whether to file STRs and to accurately implement the method of verification at the time of the transactions, through taking account of the contents of this risk assessment report[*1].

Specified business operators are required to implement appropriate initiatives based on the abovementioned revised law and take effective measures to prevent their operations from being misused for ML/TF.

Section 2. Method of Risk Assessment and Analysis of Cleared Money Laundering Cases

1. Method

For risk assessment, taking the new "40 Recommendations" etc. into account, we identified risk factors from the viewpoint of "products/services", "transaction type", "countries/regions" and "customer type". [*2]Then we analyzed the following items concerning each risk factor:

○ Inherent risk of being misused for ML/TF; and

○ Measures taken to mitigate risk (for example, legal requirements to business operators, guidance and supervision to business operators by competent administrative authorities, self-regulating efforts by industry associations, self-regulatory bodies and business operators).

The following items concerning each risk factor were also analyzed, and consequently multiple and comprehensive evaluation of each risk factor was made:

○ Situation of STRs; and

○ Cleared money laundering cases (see below 2).

For risk assessment, we used statistics, case reports etc. possessed by related ministries and agencies. Inquiries were also conducted to industry associations, self-regulatory bodies and business operators through the competent administrative authorities. The inquiry includes their AML/CFT efforts and awareness of vulnerability of transactions, products and services they handle. Regarding STRs and cleared money laundering cases, we mainly analyzed reports and cases in the past 3 years (2014-2016).

2. Analysis of Cleared Money Laundering Cases

(1) Offenders

Although offenders of money laundering vary, Boryokudan (Japanese organized crime groups), foreigners in Japan, and specialized fraud groups could be listed as major ones.

A. Boryokudan

In Japan, money laundering by Boryokudan is especially a serious threat. Among cleared money laundering cases in 2016, 76 cases (19.6 %) were related to Boryokudan members, associates and other related parties (hereinafter referred to as "Boryokudan gangsters") (see table 1).

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

Money laundering by Boryokudan gangsters seems to be carried out internationally. 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.

---

*1 For details of steps for verification at the time of the transactions, see Paragraph 10.

*2 In addition, size of specified business operators is also a factor to enhance ML/TF risks. The more transactions are conducted, the more difficult to identify and trace the criminal proceeds in transactions. In other words, the bigger the business grows, the higher ML/TF risks exist, in general. To mitigate such risks, the Act on Prevention of Transfer of Criminal Proceeds requires business operators to develop adequate AML/CFT internal control system including implementation of ongoing employee training, as a part of obligation to properly conduct CDD measures including verification at the time of the transactions . This is the approach to mitigate ML/TF risks by developing AML/CFT internal control system consistent with the size of business.

Table 1 [Number of Cleared Money Laundering Cases (Committed by Boryokudan Gangsters) under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law (2014-2016)]

Category \ Year	2014	2015	2016
Cleared cases of money laundering offenses	300	389	388
Cases by Boryokudan gangsters	60	94	76
Ratio (%)	20.0%	24.2%	19.6%

B. Foreigners in Japan

Of cleared money laundering cases in 2016, 35 cases (9.0 %) were committed by foreigners in Japan (see table 2).

Regarding money laundering by foreigners, proceeds are transferred to other countries where law systems or transaction systems are different in many cases, including a case of remitting criminal proceeds gained in Japan to foreign countries and that of remitting those proceeds gained in a foreign country to Japan

Table 2 [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 (2013-2015)]

Category \ Year	2014	2015	2016
Cleared cases of money laundering offenses	300	389	388
Cases by foreigners	36	34	35
Ratio (%)	12.0%	8.7%	9.0%

C. Specialized Fraud Group etc.

Recently, specialized fraud cases are often reported in Japan. Offenders swindle victims out of money without actually meeting them, by making phone calls etc.*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 3).

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 3 [Number of Specialized Fraud cases recognized and Total Financial Damage (2014-2016)

	2014	2015	2016
Number of recognized cases	13,392	13,824	14,154
Total financial damage (yen) (Effective total amount of financial damage)	56,550,685,877	48,197,981,078	40,765,652,881

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.

*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.

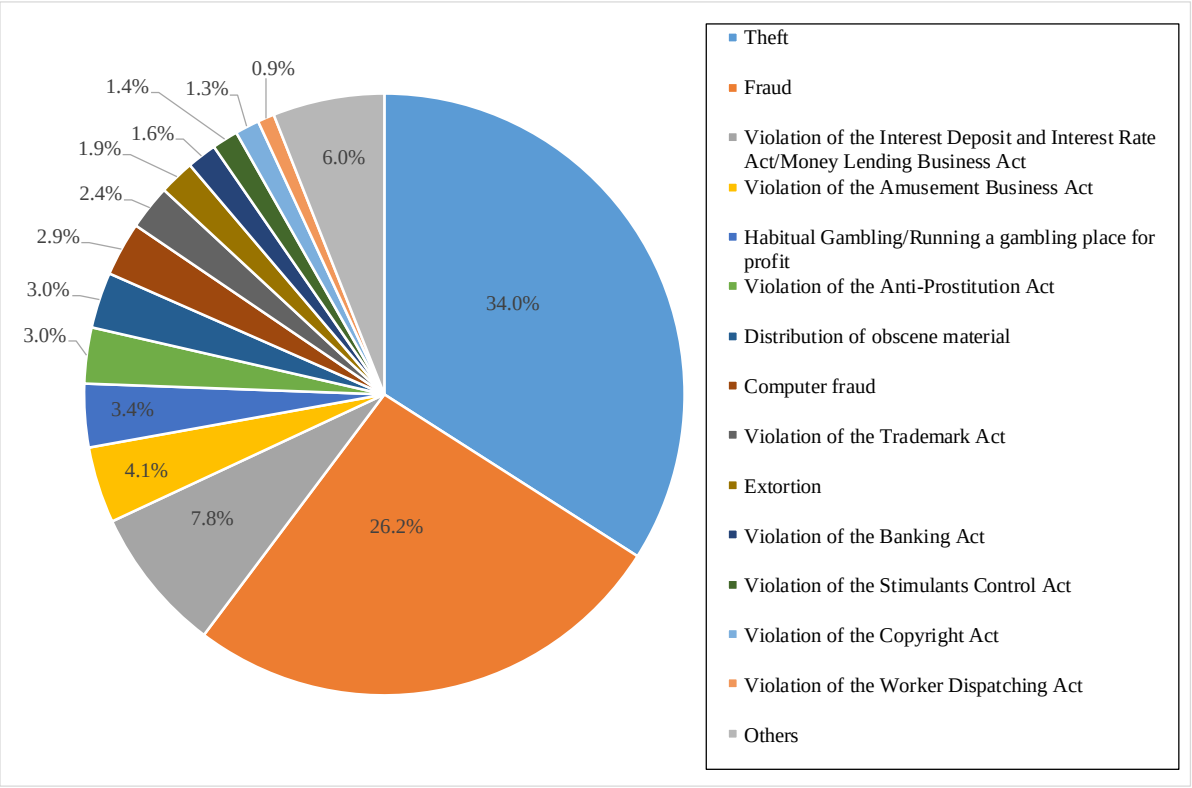
(2) Modus Operandi

A. Predicate Offenses

Money laundering offenses provided 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 predicate offenses. Predicate offenses are offences which generate illegal proceeds. They include offences 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 2014-2016, *1 theft is the leading crime with 368 cases accounting for 34.0%, followed by fraud (284 cases for 26.2%), violation of the Interest Deposit and Interest Rate Act/Money Lending Business Act (85 cases for 7.8%), violation of the Amusement Business Act (44 cases for 4.1%), and habitual gambling/running a gambling place for the purpose of gain (37 cases for 3.4%) (see table 4).

Table 4 [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 (2014-2016)]



*1 There were 1,077 cleared cases of money laundering under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law from 2014 to 2016. On the other hand, the total number of cleared money laundering cases categorized by predicate offense was 1,083 (See Table 4) because some money laundering cases can be categorized into plural predicate offenses.

Predicate offenses	Theft	Fraud	Violation of the Interest Deposit and Interest Rate / Money lending Business Act	Violation of the Amusement Business Act	Habitual Gambling / Running a Gambling Place for Profit	Violation of the Anti-Prostitution Act	Distribution of obscene materials	Computer Fraud	Violation of the Trademark Act	Extortion	Violation of the Banking Act	Violation of the Stimulants Control Act	Violation of the Copyright Act	Violation of the Worker Dispatching Act	Others	Total
Total	368	284	85	44	37	33	33	31	26	21	17	15	14	10	65	1,083
Ratio	34.0%	26.2%	7.8%	4.1%	3.4%	3.0%	3.3%	2.9%	2.4%	1.9%	1.6%	1.4%	1.3%	0.9%	6.0%	100.0%

B. Transactions etc. Misused for Money Laundering

We analyzed cleared cases of money laundering (3 years from 2014 to 2016) and counted transactions etc. which were found, in the process of criminal investigation, to be misused for money laundering. *1 *2

There were 455 domestic exchange transactions*3 and 291 cash transactions. They accounted for the majority of the transactions misused for money laundering (see table 5).

Based on the analysis of cleared cases of money laundering and STRs, we found that there are many cases where those who plan to conduct money laundering make victims pay into bank accounts opened in the name of fictitious or another party through domestic exchange transactions which enable prompt and secure fund transfer. Such criminal proceeds are often withdrawn from ATM in cash in the end, and thereafter it is very difficult to track the funds.

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

Table 5 [Transactions etc. Misused for Money Laundering (2014 – 2016)]

Misused transactions	Domestic exchange transactions	Cash transactions	Deposit transactions	International transactions (such as foreign exchange)	Precious metals and stones	Postal receiving service	Corporate status	Investment	Electronic money	Money lending	Funds transfer services	Insurance	Real estate	Legal/accounting professions	Note/check	Credit card	Safe-deposit box	Call forwarding service	Transfer of goods	Physical concealment	Total
Number	455	291	101	59	27	17	17	6	6	5	5	4	4	4	3	3	2	1	64	62	1,136

*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 There were 1,077 cleared cases of money laundering under the Act on Punishment of Organized Crimes and Anti-Drug Special Provisions Law from 2013 to 2015. On the other hand, the total number of transactions etc. misused for money laundering was 1,136 (See Table 5) because some money laundering cases can be categorized into plural transactions.

*3 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 services provided by banks and other deposit-taking institutions. Here, domestic remittances (excluding deposits and withdrawals, and the use of notes and checks) through deposit-taking institutions are counted as domestic exchange transactions.

[Supplementary Information on Method of Risk Assessment]

In conducting ML/TF risk assessment, we referred to the FATF guidance, "National Money Laundering and Terrorist Financing Risk Assessment (February 2013)." Although it is mentioned in the guidance that there is no single or universal methodology for conducting ML/TF risk assessment, a generic description of risk assessment process is indicated as follows.

○ Risk can be seen as a function of three factors: threat (meaning a person, group of people, object or activity with the potential to cause harm to the state, society, economy, etc.), vulnerability (meaning things that can be exploited by the threat or that may support or facilitate its activities) and consequence (meaning the impact or harm that ML/TF may cause). Given the challenges in determining or estimating the consequences of ML/TF, countries may opt to focus primarily on achieving a comprehensive understanding of their threats and vulnerabilities.

○ The process of identification starts by developing an initial list of potential risks to be analyzed. These will be drawn from known or suspected threats or vulnerabilities. New or previously undetected risks may also be considered at any stage. (Identification process)

○ Analysis involves consideration of the nature, likelihood, etc. of the identified risks. (Analysis process)

○ Evaluation involves taking the risks analyzed during the previous stage to determine priorities for addressing them. (Evaluation process)

In this risk assessment, we took into account of the FATF's new "40 Recommendations" and its Interpretive Notes[*1], measures under the Act on Prevention of Transfer of Criminal Proceeds, matters pointed out in the Third Round Mutual Evaluation of Japan by FATF[*2], cleared money laundering cases, etc., and took up the following materials for discussion.

○ Threats (offenders such as organized crime groups, and predicate offenses such as theft)

○ Vulnerabilities (non-face-to-face transactions, deposit/savings accounts, etc.)

We considered their

○ Impacts (amount of criminal proceeds which may be transferred, etc.)

as well, and analyzed comprehensively. Then we identified risk factors from the viewpoint of "products/services," "transaction type," "countries/regions" and "customer type."

*1 In the Interpretive Note to Recommendation 10 (Customer Due Diligence), "non-resident customers," "legal persons or arrangements that are personal asset-holding vehicles," "business that are cash-intensive," "the ownership structure of the company 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. are listed as examples of potentially higher-risk situations.

*2 In the Third Round Mutual Evaluation of Japan by FATF, it is pointed out that "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," "in case of legal persons or arrangements, there is no obligation for the financial institutions to determine who are the natural persons who ultimately own or control the customer," "financial institutions are not required to take specific steps to mitigate the increased risk accompanying dealings with PEPs," "identification and verification requirements for non-face-to-face customers are insufficient," etc.

[Amendments of Acts to reflect ML/TF risks]

This report identifies factors exerting influence on money laundering and other risks from the viewpoints of "goods and services," "countries/regions" and "customers," based on the FATF's New "40 Recommendations," findings in the Third Round Mutual Evaluation of Japan by the FATF and money laundering modus operandi measures known to us. Given these factors, Japan has revised the Act on Prevention of Transfer of Criminal Proceeds and its subordinate Order and Ordinance to impose stricter obligations on business operators to reduce risks.

Major recent revisions to the Act on Prevention of Transfer of Criminal Proceeds, etc. are as follows:

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

- Clarification of the method of making determination of filing STRs
  Specified business operators (excluding judicial scriveners, etc.) are required to make determination as to whether to file an STR through taking account of the contents of this risk assessment report, and also taking a method prescribed by the Ordinance, such as comparison with the manner of ordinary transactions, in addition to the result of CDD including verification at the time of transactions the actual manner of the transactions and other relevant circumstances.
- Verification at the time of establishing correspondent banking relationships[*1]
  When specified business operators who conduct exchange transactions on a regular basis intend to establish correspondent banking relationships with a foreign exchange transaction business operator located abroad, they are required to verify that the said foreign operators satisfies certain conditions including development of internal control systems necessary for appropriately implementing measures equivalent to verification at the time of transactions.
- Enhanced CDD when performing transactions with foreign PEPs
  Specified transactions with foreign PEPs have been added to transactions subject to enhanced CDD.
- Identification of beneficial owners
  It is required that identification of beneficial owners of legal persons reaches "natural persons" who control the legal persons through voting rights or other means.
- Method of customer identification involving identification documents without a photograph
  When identification documents without a photograph, such as health insurance certificates and pension books, are used in a customer identification process, additional identification measures are required, such as sending transaction documents to the customers' address indicated in the identification documents by registered mail requiring no forwarding, in addition to looking at the identification documents presented.
- Verification at the time of transaction where a single large transaction was divided into transactions below the regulation threshold
  When it is obvious that two or more transactions which are below the regulation threshold represent a single transaction divided in order to reduce the transaction value per transaction, they should be regarded as a single transaction.

○ Revision to the Act on Prevention of Transfer of Criminal Proceeds, etc. implemented on April 1, 2017
Virtual currency exchange business operators are added to specified business operators.

【Legal Obligations Imposed on Specified Business Operators and Case of Their Violations】

The Act on Prevention of Transfer of Criminal Proceeds and its subordinate Order and Ordinance require specified business operators to implement verification at the time of specified transaction, prepare and keep verification records and file STRs, when assets received in such transactions are suspected as criminal proceeds or when customers are suspected of committing acts amounting to the concealment of criminal proceeds. The Act also provides that competent administrative authorities shall request reports or documents from specified business operators, inspect their offices and give guidance or rectification orders as far as necessary for enforcing the Act and that the National Public Safety Commission shall provide competent administrative authorities with opinions and conduct investigations as necessary for doing so. It stipulates penalties for rectification order violations.

Between 2014 and 2016, eight rectification orders were issued under the Act (see the table below), including those on offences involving 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.

*1 Correspondent banking relationships represent contracts for continuous or repeated exchange transactions with exchange transaction business operators located in foreign countries.

○ Developing manuals to smoothly proceed with clerical work regarding the Act on Prevention of Transfer of Criminal Proceeds
○ Developing offence prevention measures and reforming practices
○ Implementing verification at the time of transaction with customers subjected to past contracts and the preparation and keeping of verification records
Specific offences found through reports collected by the National Public Safety Commission from specified business operators are as follows:

Category / Year	2014	2015	2016
Number of requests to submit reports to specified business operators	10	11	9
Number of directions to conduct inquiry to prefectural police	5	2	0
Number of opinion statements made to competent administrative authorities	11	10	8
Number of rectification orders based on opinion statements	3	5	0

【Risk Control by Business Operators (developing internal risk control arrangements based on the risk-based approach】
Regarding the abovementioned offences, specified business operators were found to have failed to develop internal control rules for the accurate implementation of verification at the time of transaction or have officials in charge of verification at the time of transaction understand relevant laws, indicating that they are required to improve arrangements for the accurate implementation of verification at the time of transaction. Given these findings, the revised Act on Prevention of Transfer of Criminal Proceeds and its subordinate Order and Ordinance, put into force on October 1, 2016, require specified business operators to take the following measures to accurately implement verification at the time of transaction:
○ Implementing employee education and training
○ Developing rules for the implementation of verification at the time of transaction
○ Appointing officials who generally manage audit and other operations to accurately implement verification at the time of transaction
○ Other measures that should be specified in rules as required under this assessment report
The revised Act also specifies the following measures to be stipulated in in-house rules:
○ Specified business operators' own risk assessment (including the preparation of forms for documents for specified business operators)
○ Collecting, putting in order and analyzing information required for measures such as verification at the time of transaction
○ Scrutinizing preserved verification and transaction records continuously
○ Acquiring approval from general managers on high-risk transactions
○ Measures required for recruiting workers with capabilities to accurately implement measures such as verification at the time of transaction
○ Conducting audit required for the adequate implementation of verification at the time of transaction
A survey on specified business operators' risk assessment found the following favorable cases:
○ Whether natural persons' professions are frequently exposed to cash handling is adopted as a risk assessment

benchmark (assessment regarding attributes of customers)

○ A wide range of information is collected on documents published by foreign public and private organizations (assessment regarding countries/regions)

○ Transactions with customers or countries/regions assessed as higher risks are separated from other transactions for a lower threshold transaction value for determining whether to file STRs to reduce risks (assessment regarding attributes of customers and countries/regions)

○ The use of goods or services assessed as higher risks are monitored and transactions with new customers in such goods or services are suspended (assessment regarding goods/services)

The extent to which risk reduction measures are implemented under risk-based approaches for specific business categories and sizes differs from business operator to business operator. It must be noted that such gap itself could become a ML/TF risk.

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. Outline of Deposit-taking Institutions

Banks and other deposit-taking institutions are required to obtain a license from the prime minister based on the Banking Act., etc. As of the end of March 2017, there were 1,394 deposit-taking institutions that had obtained a license. Among major deposit-taking institutions are banks (140 banks; excluding foreign bank branches), cooperative financial institutions (264 Shinkin banks, 151, credit associations, 13 labor banks, 758 agricultural/fishery cooperatives, and 61 federations of agricultural/fishery cooperatives). Among these institutions, banks held a total deposit balance[*3] of 737,961.6 billion yen as of the end of September 2016.

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

As to measures to contribute to mitigating risks of products and services dealt with by deposit-taking institutions, the Act on Prevention of Transfer of Criminal Proceeds imposes the obligation to conduct CDD including verification at the time of transactions on deposit-taking institutions when they provide specified products and services, as described below.

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 [*5] indicates focal points for deposit-taking institutions regarding the development of internal control systems to carry out the obligations. [*6]

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. Above all, the Japanese Bankers Association promotes organized measures against domestic and international AML/CFT issues. For example, the Association continuously studies the progress of FATF's

---

*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 "FY2016 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.

*5 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.

*6 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.

AML/CFT measures, exchanges and shares information with foreign bankers associations etc. and responds to FATF's Mutual Evaluation of Japan.

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 audit, screen out transactions that are likely to have higher risks, and adopt enhanced monitoring for transactions with higher risks.

B. STRs

There were 1,086,105 STRs by deposit-taking institutions from 2014 to 2016, accounting for 92.2% 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 (198,171 reports, 18.2%)

○ Transactions related to Boryokudan or its related parties (160,071 reports, 14.7%)

○ Transactions related to accounts to which many people frequently transfer money, especially cases where a huge amount of money is remitted or withdrawn from the account right after money is transferred in. (107,797 reports, 9.9%)

○ Transactions that deposits or withdrawals (including trade of securities, remittance, and currency exchange. 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 (66,943 reports, 6.2%)

○ Transactions that a huge amount of money is transferred from foreign countries without economic rationality (64,181 reports, 5.9%)

○ Transactions related to accounts through which a huge amount of money is frequently deposited or withdrawn (55,969 reports, 5.2%)

○ Transactions that a huge amount of money is transferred to foreign countries without economic rationality (45,353 reports, 4.2%)

○ Transactions related to accounts which usually have no fund movement, but a huge amount of money is suddenly deposited to or withdrawn therefrom (41,930 reports, 3.9%)

○ Deposits or withdrawals using accounts suspected to be opened by a fictitious or other person's name (38,469 reports, 3.5%)

○ Transactions related to accounts which have frequent remittance to many people, especially cases where a huge amount of money is deposited just before the remittance (23,570 reports, 2.2%)

○ 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 (21,892 reports, 2.0%).

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 misused as effective measures to receive and conceal criminal proceeds by those who attempt transfer of criminal proceeds.

*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.

The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct CDD including 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 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 CDD including 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. Situation of Clearance of Related Offences

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 6).

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, 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 6).

Table 6 [Number of cleared cases of violation of the Act on Prevention of Transfer of Criminal Proceeds (2014-2016)]

Year / Category	2014	2015	2016
Transfer of deposit/savings passbook, etc. (business)	19	25	29
Transfer of deposit/savings passbook, etc.	1,584	1,559	1,902
Solicitation for transfer of deposit/savings passbook, etc.	14	16	42
Transfer of exchange transaction cards, etc.	33	19	2
Others	1	0	4
Total	1,666	1,619	1,979

Note: Cleared cases in the "Others" category in 2014 and 2016 are cases of false declaration of customer identification data to specified business operators.

Table 7 [Number of cleared cases of account fraud etc. (2014-2016)]

Year / Category	2014	2015	2016
Account fraud	1,928	1,741	1,587
Receiving of stolen property	7	12	4
Total	1,935	1,753	1,591

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

c. 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.

(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 transfers of criminal proceeds could pay attention to safe and secure fund management of account and high convenience of deposit transactions and transfer criminal proceeds 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 CDD including 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 CDD including 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 fraud, embezzlement, drug crime, gambling, etc., by depositing them into accounts opened in another person's name.

(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 transfer criminal proceeds 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 CDD including 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 CDD including 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 a company manager received criminal proceeds, which were derived from underground banking business, by making the business operator remit to the company's account,

○ 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.

(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.

However, 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 CDD including 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 CDD including verification at the time of transactions the actual manner of the transactions and other relevant circumstances.

b. Case

The following is an example case 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 leased from a bank by his relative.

The following is an example case of abuse of safe-deposit boxes for money laundering abroad:

○ A case where an offender used fictitious names and made lease contracts of safe-deposit boxes with many banks to conceal criminal proceeds.

These cases show that persons involved in money laundering misuse safe-deposit boxes to physically preserve proceeds, while concealing the true user by making lease contracts of safe-deposit boxes under the name of another party.

(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.

However, bills and checks can be misused as efficient measures to receive and conceal criminal proceeds because of such characteristics. The Act on Prevention of Transfer of Criminal Proceeds requires deposit-taking institutions to conduct CDD including 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 CDD including verification at the time of transactions, the actual manner of the transactions and 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 CDD including 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.

The following are example cases of misuse of bills and checks for money laundering abroad:

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

○ A case where bills and checks were misused by a drug trafficking organization as instruments to divide and transfer a huge amount of funds.

These cases show that persons involved in money laundering misuse bills or checks for quick transfer of criminal proceeds or disguising criminal proceeds as legal funds.

D. Risk of Products and Services Dealt with by Deposit-taking Institutions

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.

However, these products and services can be convenient measures to transfer criminal proceeds because of characteristics they possess. 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 out customers and transactions related to ML/TF and eliminate them.

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

*1 Checks drawn as bearer checks stipulated in Article 5, paragraph 1, item 3 of the Check Act or checks deemed to be bearer checks pursuant to the provision of paragraph 2 or 3 of the 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 Check Act and not crossed under Article 37, paragraph 1 of the Act.

deposit-taking institutions have risks to be misused for transfer of criminal proceeds. *1 *2

In addition, based on STRs and cases, it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. (excluding the transactions specified in "Section 4 High Risk Transactions; the same applies to the following) have 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 customers who hold many accounts under different names, including names with business name)

○ 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

*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.

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

A. Present Situation

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 2017, there were 92 companies which had obtained a license from the prime minister based on the Insurance Business Act (Act No. 105 of 1995).

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires insurance companies etc. to conduct CDD including 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 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 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 CDD including 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 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 CDD including verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds.

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.

B. STRs

There were 9,045 STRs by insurance companies etc. from 2014 to 2016 (7,792 in life insurance and 1,253 in general insurance). 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 (6,471 reports, 83.0%)

---

*1 Insurance companies etc. mean operators listed in Article 2, paragraph 2, 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.

In the general insurance sector, major cases (and the number of reports) are as follows.

○ Unnatural transactions or transactions related to customers who show unnatural behavior or movements based on the knowledge and experience of staff (589 reports, 47.0%)

○ Transactions related to Boryokudan or its related parties (566 reports, 45.2%)

Furthermore, in the life insurance sector, there are a certain number of STRs focusing on payment of premium in a lot of cash (63 reports, 0.8%), 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.

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.

D. Risk

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

Actually, there are cases where illegal proceeds 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 to be misused for ML/TF.

Furthermore, based on STRs, cases, etc., it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. have higher risks.

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

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

A. Present Situation

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 futures transactions of minerals and agricultural products, as well as financial products, such as stocks, bonds, and investment trusts.

As of the end of March 2017, there were 1,946 companies which had been registered by 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 649.324 trillion yen in 2016 (see table 8).

Regarding commodity futures transactions, trading volume at commodity exchanges in Japan (Tokyo Commodity Exchange, Inc. and Osaka Dojima Commodity Exchange) is about 27.38 million contracts in 2016. Total value is about 63.0095 trillion yen in 2016, and clearing margin balance at the end of December is about 151.6 billion yen (see table 9).
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 pertaining to unclear source of funds and difficulty of tracing criminal proceeds.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires financial instruments business operators and commodity derivatives business operators, etc. who handle investment instruments to conduct CDD including verification at the time of transactions, and produce and preserve verification records and transaction records when opening accounts, when conducting transactions of financial instruments, transactions 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 CDD including 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. Comprehensive Guidelines for Supervision to Financial Instruments Business Operators and commodity derivatives business operators include focal points on the development of an internal control system regarding conducting CDD including verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds.

Japan Securities Dealers Association[*2] and The Commodity Futures Association of Japan[*3] 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.

---

*1 Financial instruments business operators, commodity derivatives business operators, etc. mean 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 Japan Securities Dealers Association is a self-regulatory organization which is 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 2017, 261 Type I financial instrument business operators join the Association and they have the obligation to comply with the rules of the Association.

*3 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 futures 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.

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 likely to have risks of ML/TF, and adopt enhanced CDD according to the degree of risks.

Incidentally, regarding investment through financial instruments business operators, etc. (securities trading and other transactions), customers are allowed to transfer funds to their own account only, not to third party, in principle. This characteristic contributes to further mitigating the risks investment has.

Table 8 [Transaction Volume of Stocks (2014-2016)]

(100 million yen)

	2014	2015	2016
First Section, TSE	5,765,250	6,965,095	6,432,058
Second Section, TSE	77,399	82,666	61,189
Total	5,842,649	7,047,761	6,493,247

Note: Data from Tokyo Stock Exchange

Table 9 [Transaction Amount of Commodity Futures Transactions (Domestic Commodity Exchanges) (2014-2016)]

		2014	2015	2016
Volume (number of contracts)	Agricultural products	901,415	1,063,389	975,802
	Minerals	21,264,522	23,748,554	26,402,832
Transaction amount (100 million yen)		656,401	622,336	630,095
Margin balance (end of December) (100 million yen)		1,455	1,332	1,516

Note 1: Data from Japan Commodity Clearing House Co., Ltd.

2: "Agricultural products" in volume column is the total transaction volume of agricultural product market, fisheries market, agricultural products index market, and sugar market. "Minerals" is the total transaction volume of rubber market, precious metals market, oil market, Chukyo oil market, and Nikkei-TOCOM Commodity Index market.

B. STRs

There were 25,211 STRs by financial instruments business operators and 41 STRs by commodity derivatives business operators from 2014 to 2016. Among cases exampled in "List of Reference Cases of Suspicious Transactions", major one (and the number of reports) by financial instruments business operators is as follows.

○ Tradings of stocks, bonds, and investments in investment trusts, etc., using accounts suspected to be opened by a fictitious or other person's name (8,613 reports, 34.2%)

Major one (and the number of reports) by commodity derivatives business operators is as follows.

○ Transactions suspected that the customer uses a fictitious or other person's name (21 reports, 51.2%)

C. Case

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

○ A case where criminal proceeds derived from fraud were invested in stocks under a relative's name.

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 futures.

D. Risk

There are many products in which investment is made through financial instruments business operators 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 and commodity derivatives business operators can be a useful measure for ML/TF.

Actually, there are cases where criminal proceeds from fraud or embezzlement in the pursuit of social activities were invested in stocks or commodity futures. Considering a relevant situation, it is recognized that investment made through financial instruments business operators and commodity derivatives business operators has risks to be misused for ML/TF.[*1][*2]

In addition, based on STRs, cases, etc., it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. have higher risks.

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

∗1 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 are made by each party, that a joint venture is established with the contributions, that the execution of business will entrusted to one or more parties in order to conduct real estate transactions, and that the proceeds generated from the said real estate transactions will be distributed, etc.) and distributes proceeds to investors, can also be a measure to make tracking criminal proceeds difficult, therefore, has risks to be misused for ML/TF.

∗2 Article 2, paragraph 2, item 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 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. Present Situation

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.

Considering these characteristics of trust, in order to protect settlors and beneficiaries by securing fair transactions including acceptance of trust, the Trust Business Act (Act No. 154 of 2004) adopts a license system (registration system is adopted for custodian type trust companies and self-settled trust companies). In addition, 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 2017, 62 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 misused for ML/TF, such as concealment of the source of illegal proceeds.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires a specified business operator who is/will be a trustee to conduct CDD including 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 CDD including 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 CDD including 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 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.

---

*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.

B. STRs

There were 74 STRs related to trusts from 2014 to 2016. *1 Among cases exampled in "List of Reference Cases of Suspicious Transactions", major one (and the number of reports) is as follows.

○ Transactions related to Boryokudan or its related parties (56 reports, 76%)

C. Risk

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. Considering a relevant situation, it is recognized that trust has risks to be misused for ML/TF.

∗1 To calculate the number, information of STRs was analyzed and relations with trusts was confirmed.

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

A. Present Situation

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 (when a company seeks to do business with sales branches and business offices in two or more prefectures, it is necessary to be registered by the prime minister). As of the end of March 2017, there were 1,865 registered companies, while the outstanding balance of loans was 21,925.2 billion yen as of the end of March 2016.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds imposes the obligation to conduct CDD including 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 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 CDD including 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 CDD including verification at the time of transactions under the Act on Prevention of Transfer of Criminal Proceeds.

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 CDD including verification at the time of transactions and STRs and prevention of damage caused by anti-social forces.

B. STRs

There were 13,039 STRs by money lenders etc. from 2014 to 2016. 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 (6,021 reports, 46.2%)

○ Deposit and withdrawal using accounts suspected to be opened by a fictitious or other person's name (3,478 reports, 26.7%)

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.

D. Risk

Money lending by money lenders etc. can make tracking criminal proceeds difficult. Considering a relevant situation, it is recognized

---

*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.

that money lending by money lenders etc. has risks to be misused for ML/TF.

In addition, based on STRs, cases, etc., it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. have 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. Present Situation

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 2017, there were 48 registered companies. There were 25.94 million remittances totaling 548.0 billion yen in fiscal 2015.

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 10).

There are three main remittance methods in funds transfer service. One is that a client brings cash to 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 an instrument (money order) correspondent to money recorded in its server and payment is done to 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.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires Funds Transfer Service Providers to conduct CDD including 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 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 CDD including 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 CDD including 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.

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 risks. Business scales of providers also vary, from major companies listed in the First Section of Tokyo Stock Exchange to small companies. Providers' internal control systems have been developed in accordance with characteristics and scales of their business.

Table 10 [Number of Performance by Funds Transfer Service（2013-2015）]

Year	2013	2014	2015
Number of remittances a year	16,819,029	20,236,0382	25,937,434
Transaction volume a year (million yen)	330,709	421,623	547,978
Number of registered funds transfer service providers	35	39	48

Note: Data from the Financial Services Agency

B. STRs

There were 1,931 STRs by funds transfer service providers from 2014 to 2016. Among cases exampled in "List of Reference Cases of Suspicious Transactions", major ones (and the number of reports) are as follows.

○ 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 (374 reports, 19.4%)

○ Transactions having unnatural aspects or conducted in unnatural frequency considering the purpose of the transactions, occupation or business of the client, etc. (276 reports, 14.3%)

○ Remittances originated from cash or checks 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) (106 reports, 5.5%)

○ Transactions related to accounts to which many people frequently transfer money, especially cases where a huge amount of money is remitted or withdrawn from the account right after money is transferred in (53 reports, 2.7%)

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 money laundering 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

*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.

remittee country through a funds transfer service provider. Among others, seeing cases of money laundering by Money Mule which misuse funds transfer service, they arise in relation with illegal money transfer involving internet banking services. For example, there are cases where offenders steal information of internet banking users by "Phishing" or by using computer viruses, then illegally access internet banking services, transfer deposit/savings money to a different account, and make Money Mule remit the money overseas by misusing funds transfer service.

D. Risk

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.

In addition, based on STRs, cases, etc., it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. have 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 Currencies Dealt with by Virtual Currency Exchange Operators

A. Present Situation

Bitcoin and other virtual currencies are known to be financial value (limited to those recorded through electronic means with electronic devices, etc., and excluding fiat currencies and currency denominated assets) that can be paid to indefinite persons for purchasing products etc.; that can be traded with indefinite persons; and that can be transferred through electronic data processing systems.

In order to engage in virtual currency exchange business, it is necessary to be registered by the prime minister based on the Payment Services Act. As of October 2017, there were 11 registered companies.

Virtual currencies have some characteristics including the transferability via the Internet. Indeed, there have been cases where virtual currencies were misused for transactions of illegal drugs or as payment for exclusive points necessary for downloading child pornography.

FATF formulated its guidance on virtual currencies in June 2015, which pointed out that users of virtual currencies are highly anonymous and that the transfer of virtual currencies, which is conducted rapidly, has borderless nature. The guidance requires each country to introduce regulations on virtual currency and fiat currency exchange operators as countermeasures against money laundering, etc.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires virtual currency exchange operators 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 currencies (conclusion of contracts concerning opening of wallets), when converting virtual currencies worth more than 2 million yen and when transferring virtual currencies of customers, etc. worth more than 100,000 yen based on the customers' request. The Act also requires the exchange operators to file an STR when the asset received in the transactions is suspected to be criminal proceeds or when their customers are suspected to be involved in the 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 CDD including 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 operator.

In addition to the supervisory measures based on the Act, the Payment Services Act stipulates that the competent administrative authorities may require the submission of reports from virtual currency exchange operators, enter their offices for inspection and issue business improvement orders etc. to them if necessary. In addition, the Payment Services Act also provides the grounds for refusing or rescinding the registration of a virtual currency exchange operator, which include "a corporation who has not established a system that is necessary for the proper and secure conducting of virtual currency exchange business." Moreover, the Guidelines for Administrative Processes by the Financial Services Agency include focal points related to the development of internal control system regarding CDD including 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 operator, 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 business." Through these measures, competent administrative authorities provide AML/CFT guidance and supervision.

B. STRs

There were 170 STRs by virtual currency exchange operators in the period between April and October 1, 2017.

C. Case

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

○ A case where an offender used a forged ID to open a wallet at a virtual currency exchange in a fictitious name and purchased virtual currencies using an illegally obtained credit card in another person's name, before converting the currencies into yen at the same exchange and having the money remitted to an account opened in a fictitious name.

E. Risk

Users of virtual currencies are highly anonymous, and the transfer of virtual currencies can be quickly conducted across national borders. In addition, the regulation of virtual currencies differs from country to country. In light of these factors, if virtual currencies are misused for crimes, it becomes difficult to trace the proceeds derived from the crimes. In consideration of actual cases where the anonymity of virtual currencies was misused to convert illegally obtained virtual currencies into cash through a virtual currency exchange operator and have the money remitted to an account opened in a fictitious name, it is recognized that virtual currencies have risks to be misused for ML/TF.

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

A. Present Situation

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 exchanging 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 11).

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 exchanging 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.

However, as to measures to contribute to mitigating risks, much of the foreign currency exchanging operator is subject to business regulations related to their main business, i.e. their obligation to obtain business license, competent administrative authorities' supervision, etc. In addition, the Foreign Exchange and Foreign Trade Act requires foreign currency exchanging operators, whose transaction volume is more than 1 million yen in a month, to report to the Minister of Finance.

The Act on Prevention of Transfer of Criminal Proceeds requires foreign currency exchanging operators to conduct CDD including verification at the time of transactions, and prepare and preserve verification records and transaction records when they make a transaction more than 2 million yen per transaction. 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 CDD including 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 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 exchanging operators if necessary.

As well, in the Foreign Exchange Inspection Manual, the Ministry of Finance 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 order to have operators fulfill their legal obligations, the Ministry of Finance prepares brochures describing outline of the report system and how to report, etc. The brochures, along with inspection manuals etc., are published on the Ministry’s website. Furthermore, the Ministry holds briefing session on revision of inspection manuals for foreign currency exchanging operators and, together with the National Police Agency, sends them a document that requires thorough implementation of CDD including 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 exchanging 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.

Some foreign currency exchanging operators make autonomous efforts against ML/TF beyond that 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.

Table 11 [Transactions by Foreign Currency Exchanging Operators (March, 2017)]

Reporter	Number of reporters (Note 3)	Number of transactions	Transaction value (1 million yen)	Value per transaction (1,000 yen)
Deposit-taking institutions				
Major banks	4	330,582	23,267	70.3
Regional banks	93	224,755	14,112	62.7
Shinkin banks	117	5,550	561	101.0
Foreign banks	15	1,149	5,953	5,181.0 (Note 4)
Other deposit-taking institutions (Note 2)	7	43,320	2,564	59.1
Excluding deposit-taking institutions				
Funds transfer service /credit card business	12	204,630	10,672	52.1
Hoteliers	49	5,531	188	33.9
Travel agencies	31	54,732	2,903	53.0
Secondhand dealers	47	67,392	4,325	64.1
Service providers related to airport	4	110,823	3,611	32.5
Large-scale retailers	4	452	11	24.3
Others	50	57,763	10,164	175.9
Total	**433**	**1,106,679**	**78,331**	**70.7**

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 1 million yen for business in February 2017 and then conducted a foreign currency exchange transaction(s) in March 2017 (pursuant to the Foreign Exchange and Foreign Trade Act, if the total transaction volume has exceeded 1 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 3,834 STRs by foreign currency exchanging operators from 2014 to 2016. 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 (1,221 reports, 31.8%)

○ 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 (992 reports, 25.9%)

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.

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.

D. Risk

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.

In addition, based on STRs, cases, etc., it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. have 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. Present Situation

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.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires financial leasing operators to conduct CDD including 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 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 CDD including 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.

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, 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 quality goods through financial leasing and allowed a head of the Boryokudan to use them for a long time.

B. STRs

There were 460 STRs by financial leasing operators from 2014 to 2016. 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 (364 reports, 79.1%)

○ 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") (34 reports, 7.4%)

○ 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") (21 reports, 4.6%)

C. Risk

Financial leasing may be made up by a lessee and a supplier in conspiracy. Considering a relevant situation, it is recognized that financial leasing has risks to be misused for ML/TF.

In addition, based on STRs etc., it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. have 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. Present Situation

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 2 months or in a revolving form. *1 As of the end of March, 2017, 258 operators were registered.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires credit card operators to conduct CDD including verification at the time of transactions, and prepare and preserve verification records and transaction records when they make 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 addition to the result of CDD including 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 conduct CDD including verification at the time of transactions and to file STRs under the Act on Prevention of Transfer of Criminal Proceeds.

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.

B. STRs

There were 37,710 STRs by credit card operators from 2014 to 2016. 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 (13,097 reports, 34.7%)

---

*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).

○ Credit card contracts suspected that the customer uses a fictitious or other person's name (11,176 reports, 29.6%)

○ Cases suspected that a person who is not a true card holder uses the credit card (5,568 reports, 14.8%)

C. Case

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

○ A case where a senior member of Boryokudan received a credit card, which was defrauded by his associate from a credit card operator, from the associate and made the associate pay for products purchased through its use.

○ 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.

.D Risk

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.

In addition, based on STRs, cases, etc., it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. have 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. Present Situation

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 These1 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 the Real Estate Brokerage Act (Act no. 176 of 1952). There were approximately 123,400 Brokers as of the end of March 2017. In 2015, the annual number of transactions was approximately 170,000, while the value of annual sales was approximately 39 trillion yen. 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.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires Brokers to conduct CDD including 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 Brokers 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 CDD including 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.

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.

B. STRs

There were 18 STRs by brokers from 2014 to 2016. 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. (5 reports, 27.8%)

○ Unnatural transactions or transactions related to customers who show unnatural behavior or attitude based on the knowledge and experience of staff (3 reports, 16.7%)

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.

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.

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

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

D. Risk

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.

In addition, based on STRs, cases, etc., it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. have higher risks.

○ Transactions in large amount 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. Present Situation

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 internationally carries precious metals weighing more than 1 kilogram, they are required under the Foreign Exchange and Foreign Trade Act and the Customs Act (Act No. 61 of 1954) to make a prior declaration to customs. However, in recent years, smuggling of gold bullion has been growing. In administrative year[*1] 2015, the number of processed cases (notifications and indictments) of gold smuggling was 294, a record high, and the value of tax evasion was approximately 610 million yen, also a record high (see tables 12 and 13).

Among the gold smuggling schemes observed in recent years are attempts to earn illegal proceeds by taking advantage of tax system differences between Japan and other countries. For example, one way to do so is purchasing gold in a country/region where no tax is imposed, smuggling it into Japan in order to evade the taxpaying obligation and selling it at a jewelry shop and the like in Japan at a price including consumption tax, thereby earning profits equivalent in value to the consumption tax. Methods of smuggling are becoming more and more sophisticated. For example, some smugglers conceal gold under their clothing, while others disguise gold as ornaments.

As for the destinations of illegal export, Hong Kong and South Korea are popular destinations. There was a case where an attempt was made to illegally export several hundred kilograms of gold bullion at a time and a case where a Boryokudan member used a private jet to smuggle gold out of Japan. These cases show that Japanese and foreign organized crime groups are involved in gold smuggling.

Meanwhile, as gold bullion prices are liable to fluctuate, cash payment is the mainstay transaction arrangement. That is one reason why gold transactions are highly anonymous.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires dealers in precious metals and stones to conduct CDD including verification at the time of transactions and prepare and preserve verification records and transaction records when they make sales contracts of precious metals and stones which exceed 2 million yen in cash. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like, 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 CDD including 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 officers, etc. may conduct on-site inspection of and issue business suspension orders to secondhand articles dealers and pawnbrokers if necessary.

Industrial associations also make efforts to promote AML/CFT measures. For example, they endeavor to raise awareness of dealers about AML/CFT by preparing manuals that explain obligations in related laws (the Act on Prevention of Transfer of Criminal Proceeds and the Secondhand Articles Dealer Act and provide trainings. In addition, the Japan Jewellery Association, 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 their websites, brochures for members, etc.

*1 An administrative year is from July to June of the following year.

Table 12 Changes in the number of processed cases of gold bullion smuggling (administrative year 2013 to 2015)

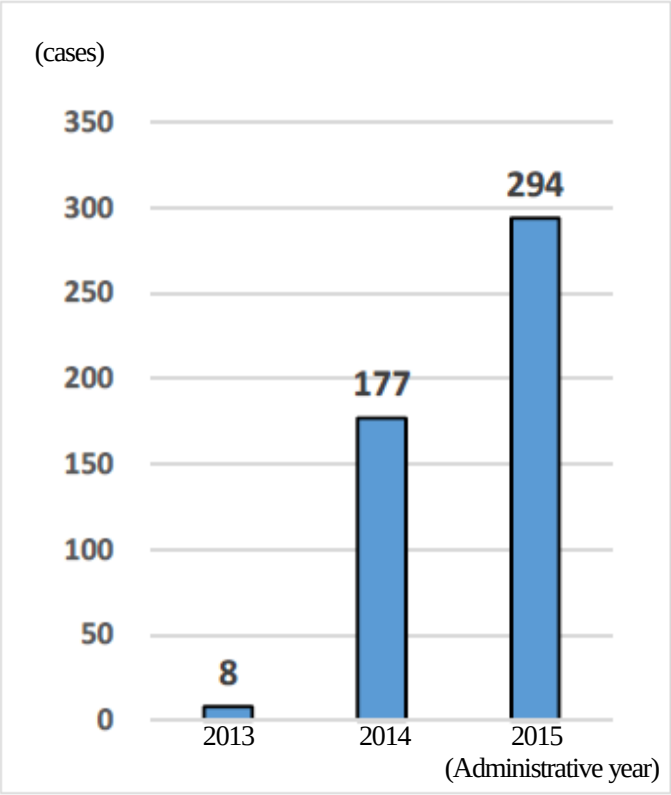
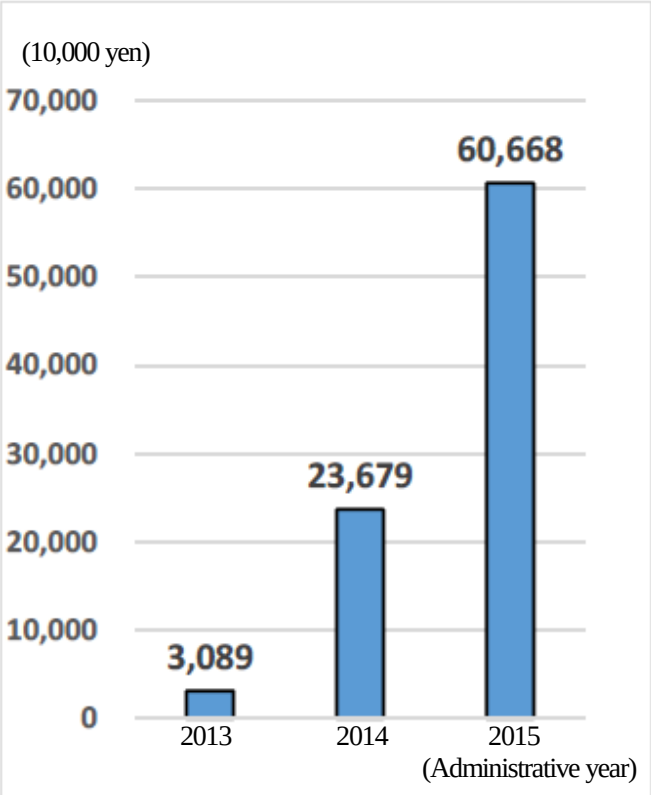


Table 13 Changes in the tax evasion amount in cases of gold bullion smuggling (administrative year 2013 to 2015



B. STRs

There were 42 STRs by dealers in precious metals and stones from 2014 to 2016. Among cases exampled in "List of Reference Cases of Suspicious Transactions", major ones (and the number of reports) are as follows.

○ Transactions in which high-value purchases are made in cash (11 reports, 26.2%)

○ Cases where several persons visit a shop at a time and request different shop clerks to conduct high-value cash transactions respectively (8 reports, 19.0%)

○ Transactions of frequent purchases resulting in a large amount, even if the purchase amount at the time is small (6 reports, 14.3%)

○ Buying and selling a lot of precious metals etc. by the same person or company in a short period (6 reports, 14.3%)

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 associate sell gold bullion obtained through theft in the name of a corporation.

○ A case where precious metals were purchased at a jewelry shop in another person's name with cash derived from theft.

These transactions were conducted with an increased level of anonymity, as the offender impersonated another person or falsified customer identification data through the presentation of forged ID at the time of the conclusion of the contract.

Meanwhile, the following is an example case abroad.

○ Cases where offenders used drug proceeds to buy gold bullion then smuggled it to a foreign country.

These cases show that as precious metals and stones are easy to carry with and have high liquidity and anonymity, they are misused for money laundering.

D. Risk

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, which means anonymity may become higher. Therefore, precious metals and stones can be an effective instrument to transfer criminal proceeds.

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.

In addition, based on STRs, cases, etc., it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. have higher risks.

○ Transactions in a large amount 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. Present Situation

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 to 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.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires postal receiving service providers to conduct CDD including verification at the time of transactions and prepare and preserve verification records and transaction records when they make service contracts. The Act also requires 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 CDD including 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.

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. In addition, the Ministry explains the Act on its website.

During the investigations related to specialized fraud, etc., suspicions of violation of the obligation for verification at the time of transactions were recognized. As a result, the National Public Safety Commission required the submission of reports from postal receiving service providers in nine cases in 2016. Specific cases of violation identified through the submitted reports are as follows:

*Neglected to verify the customer's purpose of the transaction, occupation, etc.

*Neglected to verify the corporate customer's beneficial ownership.

*Neglected to send transaction documents by registered mail in non-face-to-face transactions.

*Neglected to prepare or preserve verification records.

B. STRs

There were 64 STRs by postal receiving service providers from 2014 to 2016. 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 based on the knowledge and experience of staff (16 reports, 25.0%)

○ Contracts suspected to be made in the name of fictitious or other person's name (5 reports, 7.8%)

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.

D. Risk

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 transferor or ownership of criminal proceeds can be unclear. Therefore, postal receiving service can be an effective instrument to transfer criminal proceeds.

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.

In addition, based on STRs, cases, etc., it is recognized that transactions having the following aspects concerning circumstances at the transaction, customer types, etc. have 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.

Moreover, in light of the specific cases of violation indicated in A., postal receiving service providers' neglect to fulfill their duties under laws and regulations due to deficiencies of their internal control systems may be a factor that increases risks involved in postal receiving service.

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

A. Present Situation

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.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires telephone receiving service providers to conduct CDD including verification at the time of transactions and prepare and preserve verification records and transaction records when they make service contracts. The Act also requires 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 CDD including 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.

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

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 transferor 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 2014 to 2016.

B. Risk

Through telephone receiving service, customers can make a fictitious appearance of the business and can make a transferor or ownership of criminal proceeds unclear. Considering a relevant situation, it is recognized that telephone receiving service has risks to be misused for ML/TF.

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

A. Present Situation

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 2017, there were 787 companies which had made an application to provide telephone forwarding service.

As to measures contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires telephone forwarding service providers to conduct CDD including verification at the time of transactions and prepare and preserve verification records and transaction records when they make service contracts. The Act also requires 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 CDD including 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.

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 CDD including verification at the time of transactions and it explains the Act on its website.

STRs by telephone forwarding service providers were not made from 2014 to 2016.

B. Case

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

○ A case of concealment of proceeds from the sale of obscene DVDs where several telephone forwarding services concluded in other persons' names were misused for communication with customers.

This case shows that telephone forwarding service is misused in order to make unclear the ownership of criminal proceeds.

C. Risk

Through telephone forwarding services, customers can make a fictitious appearance of the business and can make a transfer or ownership of criminal proceeds unclear. Considering a relevant situation, it is recognized that telephone forwarding service has risks to be misused for ML/TF.

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

A. Present Situation

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, 2017, 38,980 lawyers, 9 Okinawa special members, 410 foreign lawyers, 1,035 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 roaster kept in Japan Federation of Shiho-Shoshi Lawyer's Associations. As of the end of March 2017, 22,310 judicial scriveners and 624 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, 2017, 46,205 certified administrative procedures legal specialists and 514 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 2017, 29,367 certified public accountants, 2 foreign certified public accountants, and 222 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 a certified public tax accountant roster kept in Japan Federation of Certified Public Tax Accountants' Associations. As of the end of March, 2017, 76,493 certified public tax accountants and 3,519 tax accountant 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 transfer of criminal proceeds, 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.

FATF etc. points out that with effective implementation of regulations on banks for AML/CFT those who attempt ML/TF have changed the methods. Instead of ML/TF through banks, they receive professional advice from legal/accounting professions. They also make legal/accounting professions, who have high social credibility, engage in transactions.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires legal/accounting

---

*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 tax accountant or certified tax accountant corporation) of the Act on Prevention of Transfer of Criminal Proceeds.

professions, excluding lawyers, to conduct CDD including 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 which stipulate duty of lawyers, such as verification of customer identification data in case where customers are in a specified business, preservation of verification records, and avoiding acceptance of request if there is any suspicion of being abused for criminal proceeds transfer.

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

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 unwitting tax accountant corporation was used for accounting treatment of proceeds derived from fraud in order to disguise them as legitimate business profits.

Meanwhile, the following is an example case abroad:

○ A case where a criminal drug trafficker disguised his drug proceeds as compensation money from a purchaser of a building who was an accomplice and where an unwitting lawyer was used as a transaction agent for the building.

These cases show that those who attempt money laundering misuse services provided by legal/accounting professions to disguise concealment of criminal proceeds etc. as legitimate transactions.

C. Risk

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 practical means to transfer criminal proceeds.

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.

Separate asset independent of contributors can be made in companies and other legal persons, cooperatives, and trusts. 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.

2. Products and Services Utilizing New Technology, Which Requires Further Examination of Actual State of Use etc. (Electronic Money *1)

(1) Present Situation

The average usage amount of electronic money per household a month in Japan increased from 12,480 yen in 2014 to 17,318 yen in 2016. Meanwhile, the proportion of households which used electronic money worth more than 10,000 yen increased from 20.1% in 2014 to 23.7% in 2016. In Japan, the use of electronic money has spread in the past few years (see tables 14 and 15).

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 server 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 server on network. The instruments have excellent transportability. Furthermore, in many cases, customers don't have to provide customer identification documents. Identification is completed through declaration of their 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.*2 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 In the assessment, electronic money means IC card type systems such as Edy, Suica, ICOCA, PASMO; cell phone type systems such as Osaifu-Keitai; prepaid type systems such as WebMoney, BitCash, QUO Card; and systems that money value equivalent to cash is transferred to card etc. Credit card, debit card, payment by post-paid system, and payment by prepaid card for specific products or services, such as bus card, are not included.

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

Table14【Transition of Average Usage Amount of Electronic Money per Household a Month (Households of 2 and More Persons (2014-2016)】

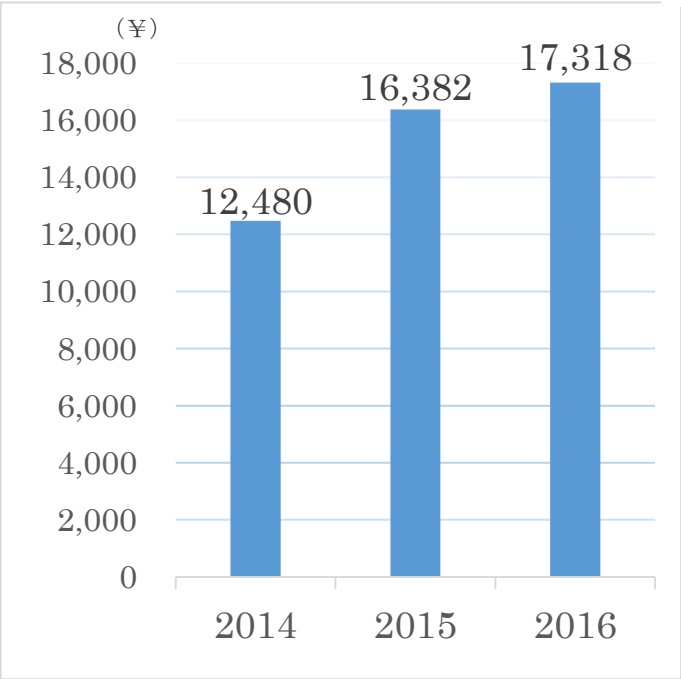
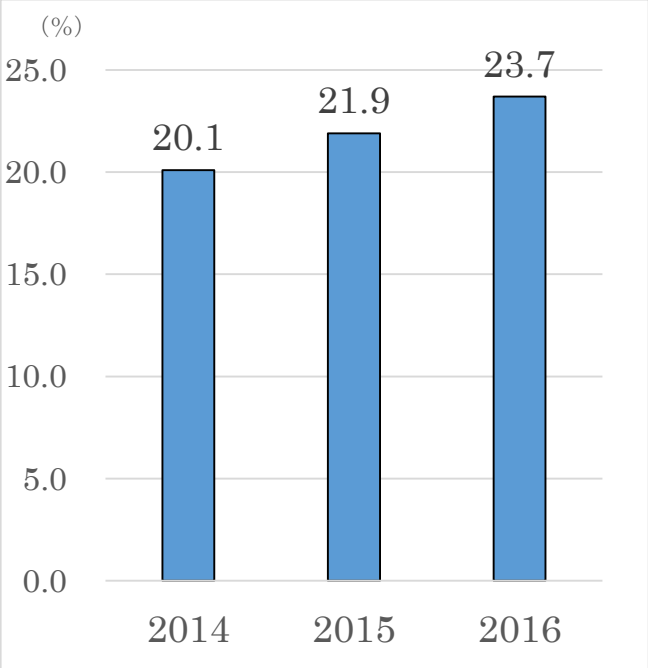


Table 15 【Transition of the Ratio of households That Used Electronic Money Not Less Than 10,000 Yen a Month (Households of 2 and More Persons) (2014-2016)】



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.

(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 an increasing number 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.

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. Present Situation

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.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds stipulates customer identification methods to be taken by specified business operators when customers' identification documents are not presented to them directly. These methods are: (i) Where specified business operators receive identification documents or the copies thereof sent from customers, and send transaction documents to the residence indicated in the identification documents or the copies thereof by registered mail requiring no forwarding or the like; (ii) postal service providers visit the residence of customers on behalf of specified business operators, verify identification documents showed by the customers and inform specified business operators of customer identification data such as name; and (iii) by electronic signature. [*1]

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 CDD including verification at the time of transaction, including CDD measures based on the fact that Internet banking is a non-face-to-face transaction.

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

[*1] In addition to regular decision-making methods, such as comparing the transaction form normally used for specified business, there are other ways for determining STRs when performing transactions with customers residing or located in a country/region that has been determined in this risk assessment report to require caution based on its development of a system for preventing the transfer of criminal proceeds or when performing transactions considered to be high risks based on the contents of this report. With respect to the measures taken for overall high-risk transactions, the Act on Prevention of Transfer of Criminal Proceeds and its Ordinance require specified business operators to:

- conduct investigations necessary to verify the questions to customers or confirm if there is any suspicious matter in the transactions; and
- get the coordinating manager (i.e., a person who coordinates and manages the audit and other duties necessary to accurately implement measures including verification at the time of transactions) or any other person equivalent thereto to verify if there is any suspicious matter in the transactions.

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.

C. Risk

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. Present Situation

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 16). Use of cash in Japan is higher than that in other countries (see table 17).

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 is highly anonymous unless they are recorded, and thus resulting in low visibility in tracing fund flow.

In the Interpretive Note to the new "40 Recommendations," FATF indicates "business that are cash-intensive" as one of the examples of potentially higher-risk situations.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators who operate financial businesses etc. to conduct CDD including verification at the time of transaction and preparation and preservation of verification records and transaction records when they conduct transactions which accompany receiving and paying cash of more than two million yen (100,000 yen in the case of a transactions which accompany exchange transactions or the writing of a cashier's check). The Act also requires specified business operators to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like, 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 CDD including 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 contribute to mitigate the risks of cash transactions.

Furthermore, competent administrative authorities provide 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 made in a huge amount of cash

○ Transactions made frequently in a short period and large in total

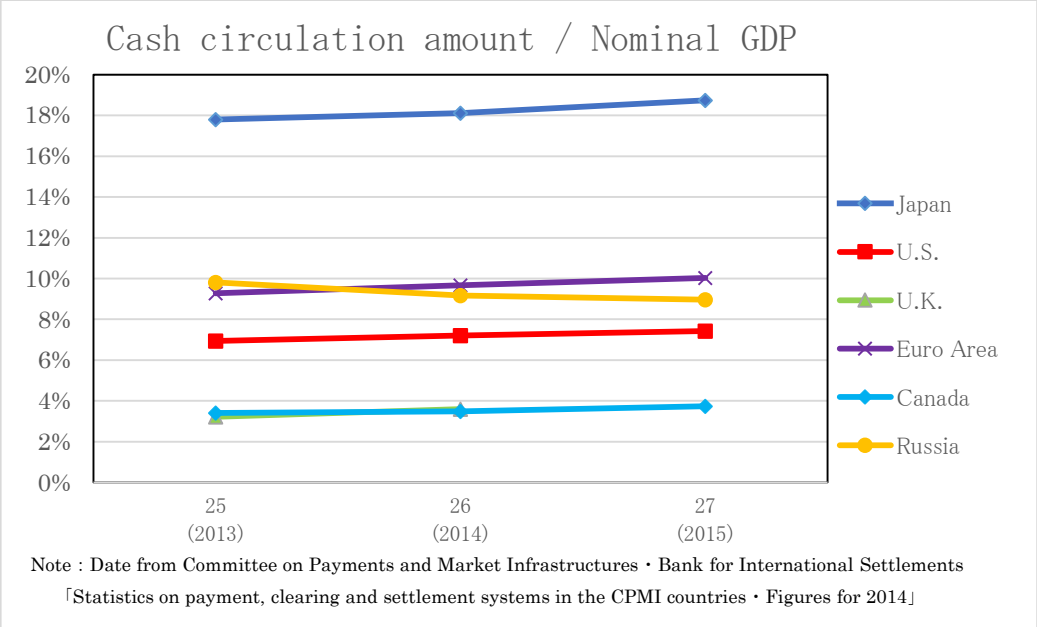
and business operators take them into account and take measures to file STRs properly.

Table 16 [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 17 [Ratio of cash distribution balance of each country in nominal GDP (2013-2015)]



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 2014」

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.

C. Risk

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. Present Situation

In 2016, Japan's economic size was the third largest in the world in terms of nominal GDP (approximately 536.8 trillion yen), the fifth largest in terms of the overall import value (approximately 66,041.9 billion yen and the fourth largest in terms of the overall export value (approximately 70,035.7 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. If a respondent institution is a fictitious bank which does not do business in fact (What is called "shell bank"), or if a respondent institution allows shell banks to use accounts, for example, foreign exchange transactions have high risks to be used to transfer or conceal criminal proceeds.

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 transfer of criminal proceeds, as well as the above-mentioned exchange transactions, etc. based on correspondent banking relationships.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires specified business operators to conduct CDD measures that they should 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. which conduct exchange transactions) have obligations, such as:

- When establishing correspondent banking relationships with a foreign exchange transaction operator, obligation to understand that the operator has an appropriate internal control system [*1] ;
- When requesting a respondent institution for a foreign exchange transaction involving remittance overseas, obligation to notify customer identification records of the originator to the institution; and
- Obligation to 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

---

[*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 CDD including verification at the time of transactions appropriately;
- Obligation to verify that the other party to correspondent banking relationships has not formed relationships for continuously or repeatedly performing exchange transactions with any financial institution etc. that does not have an internal control system necessary to conduct CDD including verification at the time of transactions appropriately; and
- Obligation to collect information on the AML/CFT systems developed by the other party to correspondent banking relationships, their business activities, and the state of supervision provided by administrative authorities of their county, and obligation to clarify the responsibility of each party in conducting CDD including verification at the time of transactions.

○ To verify that respondent institutions are not shell banks and the institutions do not allow shell banks to use accounts.

Furthermore, regarding cash couriers, when a person internationally carries cash, checks, securities, etc. over 1 million yen or precious metals over 1 kg, the person should submit written declaration to Finance Minister under the Foreign Exchange and Foreign Trade Act and to the Directors-General of Custom-Houses under the Customs Act.

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.

According to the analysis of the arrests made in money laundering cases involving visiting foreigners, Chinese, Vietnamese and Nigerian are among the top in terms of the number of arrested foreigners by nationality. By type of predicate crime, theft, fraud and violation of the Banking Act are among the top in terms of the number of arrests.

Meanwhile, the increase in the number of arrests made in cross-border money laundering cases has been particularly remarkable in recent years.

The following are example methods used in cross-border money laundering:

○ Proceeds derived from cases 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 misuse of 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, made the company remit the payment to an account opened in the name of a shell company and withdrew a large amount of cash at a time.

○ A case where proceeds (Japanese yen) derived from fraud were converted into Chinese yuan through transactions (transactions through which internet auction agency was undertaken) conducted with customers located in China.

○ 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.

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 crimes 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 comprised of visiting foreigners in Japan commit crimes upon instruction from organized crime groups located in their home countries.

In a case of Internet banking-related illegal remittance by Chinese nationals and in a case of theft of heavy construction machinery by Vietnamese nationals, the organized crime groups comprised of those foreign visitors maintained close communication with organized crime groups in China and Vietnam and divided their roles in committing the crimes.

Furthermore, there have been a succession of arrests in drug crime cases, including a case where a drug crime organization comprised mainly of Taiwanese nationals engaged in smuggling disguised as a legitimate offshore transaction, a case where a drug crime organization comprised mainly of Mexican nationals engaged in smuggling using ocean container cargoes, and a case where a large amount of drugs involving a foreign drug crime organization was smuggled into Japan. As a result, the risk is growing that proceeds derived from such smuggling activities may be recycled to other countries.

C. Risk

Compared with domestic transactions, international transactions make it difficult to track transfer of criminal proceeds because national legislation and transaction system, etc. varies from country to country.

Actually, in some cases, money laundering was conducted through international transactions. Therefore, it is recognized that international transactions have risks to be misused for 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

○ 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) Present Situation

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 November 3rd, 2017.

As to measures to contribute to mitigating risks, competent administrative authorities notified specified business operators of the statement and requested them to thoroughly implement duty of CDD including verification at the time of transaction and submission of STRs and duty 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 not sufficiently prepared (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 which involve transfer of property to a person who resides or is located in the specified jurisdictions, conduct enhanced CDD including verification of the source of wealth and source of funds as well as customer identification data etc.

(2) Risk

[*] 1 See http://www.mof.go.jp/international_policy/convention/fatf/index.html. FATF public statement is adopted in FATF plenary meeting which is held every 4 months (normally in February, June and October). Identified countries/regions could change in each time, therefore, business operators should continue paying attention to the latest statement.

As mentioned in the previous section, it is recognized that international transactions have risks to be misused for ML/TF. Based on the FATF public statements, it is recognized that transactions related to Iran or North Korea have 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 November 3rd, 2017. Even so, FATF published the names of countries/regions that have serious strategic deficiencies related to AML/CFT measures and have developed action plans to deal with 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.

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 transfer criminal proceeds:

(1) Anti-social forces (including organized crime groups) and (2) international terrorists (including Islamic extremists.)

○ Persons for which CDD is difficult to carry out:

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

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

A. Present Situation

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 or in an organized manner to gain profit.

There exist Boryokudan throughout Japan. Their size and activity vary. As of the end of October, 2017, 22 groups are listed as "designated Boryokudan gangsters" under the Act on Prevention of Unjust Acts by Organized Crime Group Members.

As of the end of 2016, total number of Boryokudan gangsters is 39,100, *2 including 18,100 Boryokudan members and 20,900 associates.

These days, Boryokudan are more careful to conceal their organizations' actual condition. They disguise their activities as business operations or claim to be a political activity or social campaign, etc. They become increasingly unclear. 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.

However, as to measures to mitigate risks, "Guideline for How Companies Prevent Damage from Anti-Social Forces" (agreed on June 19, 2007 at a working group of Ministerial Meeting concerning Measure Against Crimes) has been formulated to facilitate 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.

---

*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" racketeer, person(s) engaging in criminal activities under the pretext of social campaigns or political activities and violent groups/individuals specialized in intellectual crimes.

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

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.

B. STRs

There were 1,178,112 STRs from 2014 to 2016, including 190,298 reports (or 16.2% of total reports) related to Boryokudan gangsters.

C. Case

There were 1,077 cases cleared of money laundering from 2014 to 2016, including 230 cases (21.4% of total cases) related to Boryokudan gangsters.

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

○ Cases where Boryokudan members concealed ownership of criminal proceeds, which are from frauds including specialized frauds, 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, a contribution, etc., by taking advantage of their organizations' threat.

D. Risk

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. Furthermore, the threats of terrorism have diversified with experts pointing out the risk of fighters from different countries joining international terrorist groups and then returning to their national origins to carry out terrorist attacks. 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 the "Islamic Extremists") as customers who may become factors that affect the risks.

A. Present Situation

Terrorist attacks by Islamic extremists continue to take place all over the world, posing a serious threat. There are several groups affiliated with ISIL and AQ, mainly in the Middle East and Africa. Their main areas of activities include Iraq, Syria, Libya, Nigeria, Yemen, Afghanistan, Pakistan, Somalia and Lebanon.

The number of foreign fighters increased for reasons such as that ISIL attracted many foreign combatants from over the world by employing funds obtained through oil fields under its control and skillful media strategies. However, the number is now on a downtrend because ISIL has lost control over the region along the Turkish border that was under its control as a result of aerial bombing by the U.S.-led coalition of the willing and also because relevant countries strengthened border control. On the other hand, experts still point out that there is a risk that such foreign fighters will carry out terrorist activities in their own countries after they return home.

In addition, groups affiliated with ISIL or AQ have continued to spread their radical beliefs through the Internet, influencing those who were born or grew up in Europe, the U.S., or other non-Islamic countries to become extremists as well. These "homegrown terrorists" engage in terrorist attacks in their own countries, leading to an increase in terrorist attacks across the world.

The United Nations Security Council has adopted resolutions (No. 1267 and succeeding 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

---

*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 differences in their policies. The group took control of Mosul, a city located in the northern part of Iraq, in June 2014 and expanded the areas under its control before declaring the establishment of the "Islamic State" in areas striding 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.

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 directly.

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 currencies 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 operators 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.

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 October 20, 2017, 398 individuals and 103 groups have

been specified 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 October 20, 2017, the names of 398 individuals and 103 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.

B. Filing of STRs and Examples

Nobody has ever been arrested in connection with terrorist financing in Japan so far. However, STRs that are suspected to be 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 necessary to keep in mind the following matters in addition to the focal points related to 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.

C. 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. Present Situation

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 to be falsifying their identification data which has already been verified or when their bank accounts are suspected to be misused for ML/TF, business operators may have fewer measures to conduct appropriate CDD including verification of customer identification data, compared with customers residing in Japan.

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

As to measures to contribute to mitigating risks, the Guidelines for Supervision by the Financial Services Agency requires business operators to develop internal control systems for suitable examination and judgment to file STRs, such as comprehensive consideration of customer types and situations of transactions.

B. Risk

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. Present Situation

Foreign PEPs (Head 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 nature/ transfer of their assets are 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 asset 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.

As to measures to contribute to mitigating risks, when specified business operators conduct specified transactions with (1) the Head of State 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 verification of 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 State of a foreign country etc. listed in the Order and Ordinance.

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 of providing illicit profit to foreign public officials etc. were introduced in 1998.

Although concrete 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. Risk

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. Considering a relevant situation, it is recognized that transactions with foreign PEPs have high risks of ML/TF.

(5) Legal Persons without Transparency of Beneficial Ownership

A. Present Situation

As corporations 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 in a company, 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 property is in the complex right/control structures peculiar to legal persons. The natural person who has the beneficial ownership of the property can be easily concealed.

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 right/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 control of them, as a director).

Indeed, there are cases of fraud and violation of the Interest Deposit and Interest Rate Act where shell companies were established in order to disguise illegal activities as legitimate transactions and accounts opened in those companies' names were misused to conceal criminal proceeds.

In addition, there are cases of cross-border money laundering where accounts opened in the names of individuals using business names that include the word "trading" and the like in order to disguise illegal activity as trade transactions were used to conceal criminal proceeds and cases where a contract concerning a postal receiving service was concluded in a fictitious company's name and criminal proceeds were concealed in there.

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 circumstance, in order to prevent legal persons from being misused for ML/TF, it is important to secure transparency of legal persons and traceability of their funds, by revealing their beneficial owners.

FATF requires each country to conduct the followings.

- ○ 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.
- ○ To consider measures to facilitate access to beneficial ownership and control information by business operators.

As to measures to contribute to mitigating 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 which adopts the principle of capital majority rule, such as a joint-stock corporation; (2) a natural person who is deemed to have a right to receive dividend 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 which does not adopt the principle of capital majority rule; (3) a natural person who is deemed to have substantial impact on the business activities of a legal person; and (4) a natural person who represents a legal person and executes its business. The Act requires specified business operators to verify the identification if a 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.

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.

As to measures to contribute to mitigating risks, the Act on Prevention of Transfer of Criminal Proceeds requires the above-mentioned providers to conduct CDD including verification at the time of transactions and prepare and preserve verification records and transaction records when they make service contracts. The Act also requires them to file STRs when the property received in the transactions is suspected to be criminal proceeds or when customers are suspected to be involved in concealment of criminal proceeds and the like, 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 CDD including 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 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, 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.

C. Risk

By placing property in the complex right/control structures of legal persons, a natural person who has beneficial 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.

[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 as customer identification documents, business operators might not be able to detect a person who pretends to be another, while conducting verification at the time of transactions.

Therefore, it is recognized that non-photographic ID is vulnerable to misuse for transfer of criminal proceeds and that transactions with customers who present non-photographic ID have 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, through the 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 methods as the methods of identifying specific persons when customers submit non-photographic ID: (i) sending documents related to the transactions to the residence written on the relevant identification document by registered mail with no forwarding, (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 pay attention to cases where customers deliberately refuse to present photographic ID as cases that have the risk of misuse for transfer of criminal proceeds.

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 have low risks to be misused for ML/TF.

(i) Transactions having 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. within powers given by laws, internal control systems, etc. Process and nature of such transactions have high transparency, and a source/destination of funds is clear, so it is difficult to misuse 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 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 for ML/TF.

(v) Transactions that 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 sake have risks to be misused for ML/TF because such services may make up fictitious or exaggerated appearances of business reliability, business scale, etc. However, when services have difficulty in disguising the actual status of legal persons etc., it is difficult to misuse for ML/TF (for example, telephone receiving service which indicates to a third party that it is a telephone receiving service).

(vi) Transactions with low or no fund accumulation features

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

(vii) Transactions below the regulation 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.

Incidentally, transactions where customers are suspected that they pretend to be another person or falsify customer identification data are not considered as low risk transactions even if the transactions fall under the following transactions. Furthermore, regarding transactions prescribed by the current Ordinance as transactions that simplified CDD measures are permitted, we added applicable provisions to the following each item.

(1) Specified Transactions in Money Trust (Article 4, paragraph 1, item 1 of Ordinance)

Specified transactions in money trust including each transaction prescribed in Article 4, paragraph 1, item 1 of Ordinance (A: customer-oriented money trust with financial instruments business *1, B and D: Product client classification management trust with financial instruments business *2, C：Client classification management trust with financial instruments business *3, E：Trust contract of security deposit for issuance with issuer of prepaid payment instruments *4, F：Trust of security deposits for providing funds transfer services with Funds Transfer Service Providers *5, G：user classification management trusts with virtual currency exchange operators*6, H: Trust for preservation of deposit asset with futures commission merchant *7) fall under the transactions with factors to mitigate risks; (i), (iii), (iv) and (viii). Therefore, they are deemed to have low risks.

(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 Money etc. of Insurance Contracts That Total Repayment Is Less Than 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 Money etc. of Qualified Retirement Pension Contracts, Group Insurance Contracts, etc.

---

*1 Conclusion of a contract pertaining to a trust under Article 43-2, paragraph 2 of the Financial Instruments and Exchange Act (Act No. 25 of 1948) or establishment by the terms of trust pertaining to the trust prescribed in the same paragraph or by exercise of the right to designate beneficiary prescribed in Article 89, paragraph 1 of the Trust Act (Act No. 108 of 2006) of a legal relationship with a beneficiary of such trust.

*2 Conclusion of a contract pertaining to a product client classification management trust prescribed in Article 142-5, paragraph 1 of the Cabinet Office Ordinance on Financial Instruments Services, etc. (Cabinet Office Ordinance No. 52 of 2007) or establishment by the terms of trust pertaining to a product client classification management trust prescribed in the same paragraph or by exercise of the right to designate a beneficiary prescribed in Article 89, paragraph 1 of the Trust Act of a legal relationship with a beneficiary of such trust.

*3 Conclusion of a contract pertaining to a client classification management trust prescribed in Article 143-2, paragraph 1 of the Cabinet Office Ordinance on Financial Instruments Services, etc. or establishment by the terms of trust pertaining to a client classification management trust prescribed in the same paragraph or by exercise of the right to designate a beneficiary prescribed in Article 89, paragraph 1 of the Trust Act of a legal relationship with a beneficiary of such trust

*4 Conclusion of trust contract of security deposit for issuance prescribed in Article 16, paragraph 1 of the Payment Services Act or establishment by the terms of trust contract of security deposit for issuance prescribed in the same paragraph or by exercise of the right to designate a beneficiary prescribed in Article 89, paragraph 1 of the Trust Act of a legal relationship with a beneficiary of such trust contract of security deposit for issuance.

*5 Conclusion of trust contracts of security deposits of providing funds transfer services prescribed in Article 45, paragraph 1 of the Payment Services Act or establishment by the terms of trust pertaining to trust contracts of security deposits of providing funds transfer services prescribed in the same paragraph or by exercise of the right to designate a beneficiary prescribed in Article 89, paragraph 1 of the Trust Act of a legal relationship with a beneficiary of such trust contracts of security deposits of providing funds transfer services.

*6 Conclusion of a contract pertaining to a client classification management trust prescribed in Article 21, paragraph 1 of the Cabinet Office Ordinance concerning Virtual Currency Exchange Operators (Article Cabinet Office Ordinance No, 7 of 2017) or establishment by the terms of trust pertaining to a user classification management trust prescribed in the same paragraph or by exercise of the right to designate a beneficiary prescribed in Article 89, paragraph 1 of the Trust Act of a legal relationship with a beneficiary of such trust

*7 Conclusion of a contract pertaining to a trust prescribed in Article 98, paragraph 1, item 1 and Article 98-3 paragraph 1, item 1 of Ordinance for Enforcement of the Commodity Derivatives Act (Ordinance of the Ministry of Agriculture, Forestry and Fisheries and the Ministry of Economy, Trade and Industry No. 3 of 2005) or establishment by the terms of trust pertaining to a trust prescribed in these provisions or by exercise of the right to designate a beneficiary prescribed in Article 89, paragraph 1 of the Trust Act of a legal relationship with a beneficiary of such trust.

Payment of maturity insurance money etc. of qualified retirement pension contracts[*1] or group insurance contracts prescribed in Article 4, paragraph 1, item 3, (b) of Ordinance falls under the transactions with factors to mitigate risks;(i), (iii), (iv) and (viii). Therefore, they are deemed to have low risks.

(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.,[*2] prescribed in Article 4, paragraph 1, item 4 of Ordinance fall under the transactions with factors to mitigate risks; (iii) and (viii). Therefore, they are deemed to have low risks.

(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)

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

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

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

C. Individual Credit

Individual credit, etc. prescribed in Article 4, paragraph 1, item 6, c of Ordinance[*3] falls under the transactions with factors to mitigate risks; (viii). Therefore, they are deemed to have low risks.

(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.

Payment of entrance fees, school fees, etc. of an elementary school, a junior high school, a high school, a university, etc., prescribed

---

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

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

*3 Individual credit is a 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.

in Article 4, paragraph 1, item 7, (d) of Ordinance falls under the transactions with factors to mitigate risks; (viii). Therefore, they are deemed to have low risks.

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 prescribed in Article 4, paragraph 1, item 7, (e) of Ordinance fall under the transaction with factors to mitigate risks; (vii) and (viii). Therefore, they are deemed to have low risks.

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 CDD including 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 [*1] under the Act on Transfer of Bonds, Shares, etc., prescribed in 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 Ordinance)

Transactions in which verification is made or settlement is directed through SWIFT [*2] , 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.

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

Financial leasing transactions in which the rental fee received at one time by a lessor from a person who receives leasing services is 100,000 yen or less, prescribed in Article 4, paragraph 1, item 10 of 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 of precious metals and stones, etc. in which the payment is over 2 million yen and is made through methods other than cash, prescribed in Article 4, paragraph 1, item 11 of Ordinance, fall under the transactions with factors to mitigate risks; (viii). Therefore, they are deemed to have low risks.

(12) Specified Transactions in Telephone Receiving Service (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. [*3]) 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)

---

*1 An account which is opened in a trust bank by a company issuing shares when the company doesn't know the account of shareholders.

*2 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

*3 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.

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. Conduct 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 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, etc. that the States etc. Conduct 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.