

National Risk Assessment- Follow-up Report(2019)

Digest Version

- The National Public Safety Commission annually prepares and publishes the National Risk Assessment-Follow-up Report (hereinafter referred to as an “NRA-FUR”), which describes risks of misuse for ML/TF in each category of the transactions carried out by business operators and other matters under the Act on Prevention of Transfer of Criminal Proceeds.
- While taking into consideration the contents of the NRA-FUR, business operators file STRs after having determined whether transactions are suspicious in regard to ML/TF, and also take measures for accurately performing verification at the time of transaction, and other matters.
- This document is a digest version of the NRA-FUR published in December 2019. For more details, refer to the full version of the NRA-FUR.

Table of Contents

1. Overview of the National Risk Assessment-Follow-up Report	1
2. Analysis of Money-Laundering Cases, etc. (Offenders)	2
3. Analysis of Money-Laundering Cases, etc. (Predicate Offenses)	3 – 5
4. Risk of Products and Services	6 – 15
5. High-Risk Transactions	16 – 19

1. Overall picture of the NRA-FUR

- ✓ The NRA-FUR describes risks that products and services of business operators are misused for ML/TF, and other matters.
- ✓ While taking into consideration the contents of the NRA-FUR, business operators file STRs after having determined whether transactions are suspicious in regard to ML/TF, and also take measures for accurately performing verification at the time of transaction, and other matters.
- ✓ The following is an overall picture of the NRA-FUR, and this document provides a digest of the assessment results and analysis in "Section 2. Analysis of Money-Laundering Cases, etc.," "Section 3. Risk of Products and Services," and "Section 4. High-risk Transactions."

#	Item		Main Description
Section 1	Overview of Risk Assessment	History, Purpose, Assessment Methods	History of NRA-FUR preparation and publication; Risk assessment methods based on the FATF recommendations ; Legal obligations, etc.
		Main Contents	Results of this year's assessment; Summary regarding business operators to note and cases for them to perform ; Feedback about STRs
Section 2	Analysis of Money-Laundering Cases, etc.	Offenders	Boryokudan, Specialized Fraud Groups, and Crime groups of foreigners in Japan
		Modus Operandi	Crime forms of predicate offences and modus operandi of money laundering
Section 3	Risk of Products and Services	Major Products and Services in which Risk is Recognized	Risk factors, mitigation measures, and assessment for each product and service handled by business operators
Section 4	High-Risk Transactions	Transaction Types and Risks	Risk factors, mitigation measures, and assessment for each transaction type
		Countries/Regions and Risks	Risk factors, mitigation measures, and assessment related to countries/regions that affect the risks of transactions
		Customer Attributes and Risks	Risk factors, mitigation measures, and assessment for each customer attribute that affect the risks of transactions
Section 5	Low-risk transactions	Factors that Mitigate Risks	Transactions with factors that mitigate risks in the light of customer/transaction types, settlement methods, legal systems, etc.
		Low-risk transactions	Specific transactions that have factors to mitigate risks

2. Analysis of Money-Laundering Cases, etc. (Offenders)

2

- ✓ Although there are various types of perpetrators who engage in money laundering, Boryokudan (Japanese organized-crime groups), specialized fraud groups, and crime groups of foreigners in Japan are considered to be the main offenders. The following is an overview of the assessment and analysis results for each of these groups.

Offenders	Assessment and Analysis Results
Boryokudan	<ul style="list-style-type: none">• Boryokudan commit crimes professionally to gain economic profit and are skilled at money laundering, etc., posing a serious threat as money launderers in Japan.• In addition, the majority of cleared cases of Boryokudan involved in predicate crimes of money-laundering crimes in the last three years have been for fraud and theft. It also appears that Boryokudan gangsters have been heavily involved in gambling and prostitution offenses.
Specialized Fraud Group	<ul style="list-style-type: none">• Special fraud is the collective term for offenses that involve defrauding the victim of cash or other valuables by phone calls to an unspecified large number of persons and gaining their trust without meeting them in person, thereby persuading them to transfer money into a specified savings account, or through other methods. This type of crime has been occurring often in recent years.• With a ringleader as its core, a specialized fraud group assigns a role to each member. For example, one member cheats victims, another withdraws money, and the other procures tools to commit the crime. In this way, they commit organized fraud. In addition, they launder money, for example, by using bank accounts in the name of fictitious or other parties as a means to receive money from a victim. The number of recognized specialized fraud cases and the total financial damage were 17,844 cases and approximately 38.3 billion yen, respectively, in 2018.• There are some people who thoughtlessly sell their own bank account to obtain funds for amusement expenses or the cost of living. Some even make bank accounts in the name of fictitious or third parties by using falsified ID cards and selling them. Such people make money laundering easier.
Crime groups of foreigners in Japan	<ul style="list-style-type: none">• Criminal proceeds from offenses that involve foreigners are difficult to trace. This is because there are different legal and transactions systems. Such crimes also have characteristics that their human networks, manner of offenses, etc. are not limited within one country and that offenses tend to be more sophisticated and hidden, as the roles of offenders are divided across borders.• Observations of the situation indicate that money-laundering offenses are committed in organized-crime operations by foreigners in Japan, and there were money-laundering offenses associated with cases of illegal remittance offenses pertaining to Internet banking systems by a group of Chinese, shop-lifting offenses by a group of Vietnamese, and international fraud offenses by a group of Nigerians.

3. Analysis of Money-Laundering Cases, etc. (Predicate Offenses): 1/3

- ✓ The size of generated criminal proceeds, relevance to money-laundering offenses, etc., types of misused transactions, danger of fomenting organized crime, and impact on sound economic activities, etc. differ depending on the type of predicate offense to money laundering.
- ✓ The following is an overview of the assessment and analysis results for main predicate offenses.

Predicate Offenses	Assessment and Analysis Results	
Theft	Forms of offenses	<ul style="list-style-type: none"> • The forms of theft offences are diverse. Generally, there are cases where the amount of financial damage is comparatively small, but there are also cases committed professionally and repeatedly by crime organizations such as Boryokudan and crime groups of foreigners in Japan that result in large amounts of criminal proceeds. The total financial damage from theft during 2018 was about 58 billion yen.
	Modus operandi of money laundering	<ul style="list-style-type: none"> • A large number of coins obtained via burglary were deposited into and withdrawn from an account of another party, resulting in factual exchange; a large quantity of stolen gold ingots was sold to a gold trader in the name of a corporation operated by a friend of the offender; and goods were purchased on the Internet using cash-card information obtained illegally and received by designating addresses of fictitious persons or addresses other than actual residences as the destinations, etc.
Fraud	Forms of offenses	<ul style="list-style-type: none"> • Fraud offenses, including specialized fraud offenses, have been professionally and systematically committed by domestic and foreign criminal groups. The financial damage from fraud during 2018 was about 62.3 billion yen.
	Modus operandi of money laundering	<ul style="list-style-type: none"> • In many cases, damage from specialized fraud offenses are transferred to bank accounts in the name of fictitious or other parties. Also, there is a tendency that the criminal proceeds transferred to such accounts are withdrawn immediately after the transfer, remitted to other accounts, or transferred through multiple accounts opened under another person's name. This is done to avoid financial institutions or the like freezing accounts once they have detected the damage. • Holders of accounts used for concealment differ depending on the form of the offence; they may be individual persons, corporate bodies, or individual persons accompanied by a business name. There have also been cases where business operators of postal receiving services or call forwarding services did not sufficiently follow their customer verification obligations, and as a result were misused as a way to conceal crime organizations committing specialized fraud offenses, etc.

3. Analysis of Money-Laundering Cases, etc. (Predicate Offenses): 2/3

Predicate Offenses	Assessment and Analysis Results	
Computer fraud	Forms of offenses	<ul style="list-style-type: none"> Computer fraud is committed to remit the criminal proceeds generated from specialized fraud and illegal Internet banking, etc. One example of this form of specialized fraud is using cash cards, obtained through cheating victims, to illegally obtain cash by transferring criminal proceeds to accounts in another party's name via an ATM. In terms of illegal remittance offenses related to Internet banking, there were cases where illegal remittances were made from other parties' accounts by illegally accessing the business system managed by financial institutions using IDs, passwords, etc. of other parties.
	Modus operandi of money laundering	<ul style="list-style-type: none"> There were cases where the maximum amount of cash was withdrawn from ATMs using cash cards obtained via specialized fraud offenses, and the maximum amount for transfer was remitted to accounts in names of other persons. Also, a crime organization in China illegally accessed the business system of a financial institution in Japan and illegally remitted money to an account in the name of another person, and a criminal group of Chinese in Japan withdrew cash from the account.
Violation of the Investment Act/ Money Lending Business Act	Forms of offenses	<ul style="list-style-type: none"> This is a form of loan-shark crime whereby a money lending business operates without a license and lends at a high interest rate. Cases include instances of lending without the lender and borrower directly meeting, where the borrower returns money by transferring it to an account in the name of another party. Lenders may send direct mail based on lists of heavy debtors
	Modus operandi of money laundering	<ul style="list-style-type: none"> There have been cases where debt repayments were remitted to accounts in the name of another party to conceal debt repayments to the loan-shark offenders. These accounts were obtained by the loan-shark offenders as debt repayments from borrowers and illegally used to conceal criminal proceeds.
Habitual gambling/ Running a gambling place for profit	Forms of offenses	<ul style="list-style-type: none"> In addition to "flower card" gambling, baseball gambling and game-machine gambling, there are various forms such as online casino gambling. The reality is that Boryokudan are directly or indirectly deeply involved in those gambling offenses, and gambling is an important source of funds for them.
	Modus operandi of money laundering	<ul style="list-style-type: none"> In addition to a gambling offense committed by an online casino in which money bet by betters had to be paid to an account opened in another person's name, and there were cases of gambling offenses related to baseball gambling, etc. in which dividends were transferred to accounts in other persons' names.

Predicate Offenses	Assessment and Analysis Results	
<p>Violation of the Amusement Business Act/ Violation of the Anti-Prostitution Act</p>	<p>Forms of offenses</p>	<ul style="list-style-type: none"> It is recognized that Boryokudan have been directly or indirectly involved in certain cases, such as association with operators of illegal adult-entertainment businesses, etc. Criminal proceeds from amusement-related offenses are important sources of funds for them. There are certain cases where foreigners who are living illegally in Japan work illegally in adult-entertainment business, etc.
	<p>Modus operandi of money laundering</p>	<ul style="list-style-type: none"> There were cases where sales proceeds paid by credit cards were transferred to a bank account in the name of another party, and where a Boryokudan member received proceeds from prostitution through a bank account in the name of a family member.
<p>Narcotics-related crimes</p>	<p>Forms of offenses</p>	<ul style="list-style-type: none"> Regarding stimulant-related crimes, which account for more than 70% of all narcotics-related crimes, the amount of stimulants confiscated exceeded 1,000 kilograms for three consecutive years from 2016 to 2018, and it can be assumed that smuggling and illicit trafficking of stimulants generates a large amount of criminal proceeds. It is recognized that narcotics-related crimes are one of the major sources of funds for Boryokudan gangsters, etc. Evidence gathered in recent years strongly suggests that Boryokudan collude with overseas drug-related crime organizations, and have been deepening their involvement in the distribution of stimulants. Chinese, Mexican and West-African organizations, in particular, have been continuing to increase their presence, and criminal proceeds from drug-related crimes are important sources of fund for overseas crime organizations as well.
	<p>Modus operandi of money laundering</p>	<ul style="list-style-type: none"> There have been many cases where payment was concealed by remitting it to an account under the name of another person. There has also been a case where suspicious fund transfers involving a bank account under the name of a relative of a Boryokudan member, which led to an investigation that cleared a case of stimulant smuggling following the arrest of the Boryokudan member and other members as well. Automobiles, land, buildings, etc. were targeted for temporary restraining order for confiscation before the institution of prosecution based on the previous Anti-Drug Special Provisions Law, and it is recognized that the proceeds from drug crimes obtained using cash, etc. have changed in form.

4. Risk of Products and Services: 1/10

- ✓ Specified business operators are required to implement appropriate measures based on the Act on Prevention of Transfer of Criminal Proceeds in order to prevent products and services they handle from being misused for ML/TF.
- ✓ The following is an overview of risk assessment for each product and service handled by specified business operators, transactions that increase risk, and measures taken to mitigate risks.

(1) Products and Services Dealt with by Deposit-taking Institutions

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> • Deposit-taking institutions provide various products and services, including accounts that guarantee safe fund management, deposit transactions for quick preparation or storage of funds regardless of time and place, exchange transactions for transferring funds from one place to another or to many people quickly and securely, safe-deposit boxes for safe storage of property while maintaining secrecy, and bills and checks that are negotiable and easy to transfer. • On the other hand, those same characteristics of financial products and services can make them convenient for transferring criminal proceeds. Actually, there are cases where accounts, deposit transactions, exchange transactions, safe-deposit boxes, bills and checks have been misused to receive or conceal criminal proceeds. As such, it is recognized that products and services of deposit-taking institutions present risks of misuse for money laundering. Furthermore, based on the status and role of Japan as an international financial market, the large financial transaction volume of the industry as a whole, statistics of transactions misused for ML/TF, occurrences of cases where cross-border crime organizations are involved, and so on, the risk of misuse for money laundering is considered to be relatively high in comparison with other types of businesses.
Transactions that increase risk	<ul style="list-style-type: none"> • Transactions related to accounts that usually show no movement of funds, but a large amount of money is suddenly deposited into or withdrawn from them • Transactions conducted in an unusual manner and with an unusual frequency in light of the purpose of transactions and the occupation or the contents of business that were verified at the time of opening the account • Deposits, withdrawals, etc. using accounts suspected of being opened in a fictitious or other person's name
Measures by business operators	<ul style="list-style-type: none"> • Cases where misuse of bank accounts is prevented by stopping accounts in which deposit and withdrawal transactions are absent for a long time and checking the principal identification documents, passbooks, etc. of customers who wish to resume • Cases of banks that have an internal regulation system whereby accounts opened with a small amount of money, accounts of persons who live in a remote area, or accounts of corporations that have just relocated or been established, etc., are designated as accounts targeted for control. If any request for a transfer to such accounts occurs, the consistency of such request with the purpose of opening the account is checked and the intent of the person requesting the transfer is checked, and if the consistency cannot be confirmed, the transaction is denied or the transaction is reported as suspicious • Cases of checking the visa length of customers who are foreign students or workers, and using a system to control the risk of sale of accounts at the time of their return home

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

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> • Since insurance products with cash accumulation features enable ML/TF to be converted to immediate or deferred assets, they can be a useful measure of ML/TF. • Actually, there are cases where money laundering related to violation of the Anti-Prostitution Act were used to buy insurance products with cash accumulation features. Considering this relevant situation, it is recognized that such insurance products have risks that can be exploited for ML/TF.
Transactions that increase risk	<ul style="list-style-type: none"> • Transactions related to contractors who pay premiums in large amounts of cash
Measures by business operators	<ul style="list-style-type: none"> • Cases where the inherent risk associated with cash transactions is regarded as high risk and thereby the receipt of cash for insurance premiums, repayment of loans to policyholders, etc. is canceled; as a rule, cashless insurance payment is also promoted by making payments to the accounts of the principals for which money is held; when a cash transaction exceeds a certain amount, a questionnaire, etc. using specified check sheets, etc. is conducted and the approval of a supervisor is required; and transaction conditions, etc. are captured by the system in order to manage them after the fact

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

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> • There are many products in which investment is made through financial instruments business operators, etc. and commodity derivatives business operators. And it is possible to convert proceeds derived from crimes to various rights and commodities through these products. • In addition, some of these investment products involve complex schemes that can make tracking sources of invested funds difficult. Therefore, they can be a useful way to launder money.
Transactions that increase risk	<ul style="list-style-type: none"> • Transactions where it is suspected that the customer is using a fictitious or other person's name
Measures by business operators	<ul style="list-style-type: none"> • Measures include establishing and strengthening AML/CFT internal control systems of business operators. For example, they have set up divisions in charge, developed their own rules and manuals, and provide periodic training, conduct internal audits, screen out transactions that are likely to pose ML/TF risks, and rigorously conduct CDD. • Measures include prohibiting cash transactions as a way to mitigate such risks is recognized as an example of risk assessment and an effort by business operators to implement the risk-based approach, etc.

(4) Trusts Dealt with by Trust Companies

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> Trusts have the functions of transferring property rights from a settlor to a trustee, changing the nominee of the property when it is subject to a registration system, and altering the attribution, quantity and nature of the property. Furthermore, trusts can come into force on conclusion of a trust contract between parties involved or as a self-settled trust. Because of such characteristics, offenders attempting ML/TF may be able to separate themselves from criminal proceeds and conceal the relationship with the proceeds if they misuse a trust. No cleared money-laundering case involving misusing trusts has been reported in Japan in recent years. However, these characteristics mean that trusts can be considered as risky for misuse in ML/TF.
Measures by industry association	<ul style="list-style-type: none"> Measures include supporting AML/CFT activities conducted by each business operator by providing training and a range of information from external consulting companies through business communication meetings and study-group meetings on money laundering. The Association explains to each operator the details to be described and points for verification in the document prepared by specified business operators according to the intention of the respective member company, and shares opinions about establishing systems for AML/CFT measures.

(5) Money Lending Dealt with by Money Lenders, etc.

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> Money lending by money lenders, etc. can make tracking criminal proceeds difficult. Considering a relevant situation, it is recognized that money lending by money lenders, etc. carries the risk of misuse for ML/TF.
Transactions that increase risk	<ul style="list-style-type: none"> Money-lending contracts in which it is suspected that the customer is using a fictitious or other person's name
Measures by industry association	<ul style="list-style-type: none"> Measures include developing self-regulating rules that require member companies to establish internal control systems by means of making each company's internal rules about the obligation to conduct verification at the time of transactions, file STRs when necessary, and prevent damage caused by anti-social forces.

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

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> • Considering characteristics of foreign exchange transaction business and the fact that some funds transfer service providers provide services to remit to many countries, funds transfer services can be a useful measure for ML/TF. • Actually, there have been cases where criminal proceeds were transferred overseas through funds transfer services by using third parties who were not involved in predicate offenses or by using another person's ID to pretend to be the person. Considering these situations, it is recognized that funds transfer services present risks of misuse for ML/TF. • In light of the fact that both the number of remittances per year and the amount handled per year by fund transfer service providers are increasing, the fact that their use is expected to increase due to the increasing number of foreign residents in Japan indicates that the degree of risk that fund transfer services present in terms of misuse for money laundering, etc. is growing relative to other business categories.
Transactions that increase risk	<ul style="list-style-type: none"> • Transactions conducted in an unusual manner and with an unusual frequency in light of the purpose of transactions and the occupation or the contents of business that were verified at the time of opening the account • 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, the risk is recognized as being particularly high) • Transactions in which deposits and withdrawals are made in large amounts of cash or checks (in cases of transactions that are made in large amounts and are disproportionate to the customer's income or assets, and transactions in which cash is deposited or withdrawn even though it is considered more appropriate to use a remittance or a cashier's check, the risk is recognized as being particularly high)
Measures by business operators	<ul style="list-style-type: none"> • Cases where upper limits are set for transaction amounts according to the product/service, transaction type, country/region, or customer attributes, and transactions exceeding those amounts are severely scrutinized (for example, upper limits for transaction amounts vary depending on visa status, such as permanent resident, technical intern, student studying abroad, etc.) • Cases where a resident card is presented as the principle identification document to confirm the period of stay and its period is controlled by using system when conducting a transaction with a foreigner • Cases where risk is evaluated for each customer by taking into account the customer attributes and transaction conditions, and measures are taken according to the evaluation

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

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> • Important characteristics of virtual currency are that its users are highly anonymous and that the transfer of virtual currency can be quickly executed across national borders. In addition, regulation of virtual currency differs from country to country. In light of these factors, if virtual currency is misused for crimes, it becomes difficult to trace the proceeds derived from the crimes. • Considering actual cases where the anonymity of virtual currency was misused to convert illegally obtained virtual currency into cash through a virtual currency exchange service provider and have the money remitted to an account opened in another person's name, it is recognized that virtual currency is at risk of being misused for ML/TF. • And, considering that virtual currency transactions are increasing globally and the environment surrounding such transactions is rapidly changing, it is recognized that the level of risk for misuse of virtual currency for ML/TF, is relatively high in comparison to other types of business. Furthermore, since the deposit-taking institutions are strengthening their AML/CTF countermeasures, there are concerns that persons attempting to conduct ML/TF will use virtual currency transactions in lieu of goods and services handled by the deposit-taking institutions. This situation is increasing the degree of risk associated with virtual currency. • It is not easy to take appropriate and timely risk-mitigating measures amid rapid changes in the environment surrounding virtual currency transactions, and if such efforts are insufficient, appropriate mitigating measures cannot be taken and the degree of risk will remain high.
Measures by business operators	<ul style="list-style-type: none"> • Cases where information or data such as the number of legal person and individual customers, percentages of customers' countries of residence and countries of origin, and types of virtual currency and legal tender handled are taken into account in the business operators' own feature analysis • Cases where risks associated with the deposit route of legal currency are identified and evaluated, and in light of such risks, measures to mitigate risks such as restricting the payment and funds-transfer frequency for a certain period for deposits made at convenience stores • Cases where a business operator monitors transfer destination addresses by using a virtual currency analysis tool in light of risks associated with the transfer of virtual currency, and for an attribute determined as high risk, it takes risk mitigation measures such as restricting transfers

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

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> Foreign-currency exchange can be a part of a strategy to take the proceeds of crime. Foreign-currency exchange is usually carried out in cash, which is highly liquid and can be possessed or transferred without information about the bearer. As such, foreign-currency exchange can be a useful way to launder money or finance terrorism Actually, there has been a case where foreign currency obtained as criminal proceeds of crime committed overseas was converted to Japanese yen through a third party who did not know the actual circumstances. Considering this relevant situation, it is recognized that foreign-currency exchange carries risks of misuse for ML/TF.
Transactions that increase risk	<ul style="list-style-type: none"> Transactions large amounts of cash and frequent transactions in a short period Transactions in which it is suspected that the customer intentionally avoided verification at the time of the transactions, and transactions in which it was suspected that the customer was acting on behalf of other people, etc.
Measures by business operators	<ul style="list-style-type: none"> Cases where transactions for certain amounts are classified as high-risk transactions and, if such transactions occur, measures such as reports to the headquarters and execution of necessary research are specified in internal Cases where, considering risks in which a large transaction is intentionally separated into two or more smaller transactions for the purpose of avoiding verification at the time of transaction, verification at the time of transaction is conducted based on a threshold value which is independently specified internally, and the results are saved into a database, and monitored to check whether there are any customers conducting transactions in large amounts in total

(9) Financial Leasing Dealt with by Financial Leasing Operators

Item	Analysis Results
Assessment of risks	<ul style="list-style-type: none"> Although there were no cleared money-laundering cases involving the misuse of financial leasing, because finance leases have the characteristic of a lessee and a seller being able to conspire to conduct a false transaction, it is considered that finance leases are at risk of being misused for ML/TF.
Transactions that increase risk	<ul style="list-style-type: none"> Transactions related to financial leasing in which it is suspected that a lessee and a supplier conspire with the intent to defraud a financial leasing operator out of money by pretending to install equipment, etc.
Measures by industry association	<ul style="list-style-type: none"> Support is available for AML/CFT measures taken by financial leasing operators. For example, leaflets and brochures are prepared and distributed to provide operators with an outline of the Act on Prevention of Transfer of Criminal Proceeds and verification items at the time of transactions, and training, etc. is provided.

(10) Credit Cards Dealt with by Credit Card Operators

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> • Credit cards allow a holder of criminal proceeds in cash to transform them into different kinds of property. It is also possible to transfer funds by providing a credit card to a third party and making him purchase products. Considering this, it is recognized that credit cards present the risk of misuse for ML/TF.
Transactions that increase risk	<ul style="list-style-type: none"> • Credit card contracts in which it is 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 using credit cards, etc.
Measures by business operators	<ul style="list-style-type: none"> • Cases where transactions to purchase negotiable merchandise, such as gift certificates, during a short period are specified as high-risk transactions and, if such transactions are detected by a monitoring system, the credit card function is suspended, and a telephone call is made to the card holder to check the details of use or the user • Cases where the increase in the credit limit of a credit card is not permitted in principle until one year has elapsed since the application, in order to mitigate the risks by a person attempting money laundering using a contracted card

(11) Real Estate Dealt with by Real Estate Brokers

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> • Real estate has high value and can be exchanged for large amounts of cash. Furthermore, it is possible for offenders to transfer criminal proceeds by, for example, paying more than the market value for a property. From these aspects, real estate can be a convenient instrument for ML/TF. • Actually, there have been some cases where criminal proceeds from prostitution or fraud were used to buy real estate. Considering this, real estate presents a risk of misuse for ML/TF.
Transactions that increase risk	<ul style="list-style-type: none"> • Transactions large amounts of cash or other transactions suspected to have been conducted under a fictitious or other person's name
Measures by business operators	<ul style="list-style-type: none"> • Cases where information on transactions with customers for whom transactions were cancelled or transactions were not performed for any reason in the past placed into a database for employees in the company to share and, if any subsequent transactions with such customers occur, measures are taken to strengthen customer management or to reject those transactions

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

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> Precious metals and stones have high value and are distributed all over the world. It is easy to exchange them for cash or carry them around. In addition, the difficulty of tracking their distribution channels and locations after purchase and sale gives them high anonymity. In particular, gold bullion transactions are mainly conducted through cash payment, meaning anonymity may increase even higher. Therefore, precious metals and stones can be an effective instrument for laundering money. Actually, there are cases where offenders pretended to be another person and bought precious metals with cash derived from crimes. Considering this, precious metals and stones present a high risk of misuse for ML/TF. Taking into account the crimes committed in relation to gold bullion in recent years, it is believed that the risk in which gold bullion is misused for money laundering is increasing.
Transactions that increase risk	<ul style="list-style-type: none"> The same person/company buying and selling a large amount of precious metals in a short period Transactions in frequent purchases resulting in a large amount, even if the purchase amount at the time is small Purchases or sales with high value that are not proportionate to the customer's income, assets, etc.
Measures by industry association	<ul style="list-style-type: none"> Measures taken on gold bullion transactions include requesting operators to check declaration forms and tax payment receipts at Customs for gold bullion brought in from abroad, to preventing the purchase of smuggled gold bullion. Measures include: efforts to improve the level of understanding of business operators, etc. about money laundering, etc. by creating and distributing leaflets and booklets that give an overview of the Act on Prevention of Transfer of Criminal Proceeds and the details of obligations that business operators must fulfil; holding briefing sessions on AML/CFT measures; and creating websites, etc. to communicate the information. Measures include: communicating AML/CFT measures to all business operators by creating manuals summarizing the idea of performing obligations under the related laws (Act on Prevention of Transfer of Criminal Proceeds and Secondhand Articles Dealer Act); and holding training sessions to promote initiatives for preventing ML/TF

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

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> Postal receiving services are misused to provide locations for sending proceeds derived from crime, such as fraud and sales of illegal goods. If falsified customer identification data is provided to conclude a service contract, it can be difficult to identify the party committing the ML/TF offence or ownership of who owns the criminal proceeds. Therefore, postal receiving services can be an effective instrument for ML/TF. Actually, there are cases where offenders made contract with postal receiving service providers under fictitious names and deceived the providers into receiving criminal proceeds through concealment. Considering this, it is recognized that postal receiving services present a risk of misuse for ML/TF.
Transactions that increase risk	<ul style="list-style-type: none"> Transactions with a customer who plans to make contracts of a postal receiving service using multiple companies' names
Measures by business operators	<ul style="list-style-type: none"> Cases where information on customers with whom transactions were cancelled or could not be achieved in the past for any reason is shared among other companies in the same industry to strengthen customer control

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

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> Recently we have not seen any cleared cases for money laundering involving misuse of a telephone receiving service. However, since telephone receiving services have the characteristic of enabling customers to create a fictitious appearance for their business and to disguise the principal of an ML/TF operation and the ownership of criminal proceeds unclear, it is considered that telephone receiving services present a risk of being misused for ML/TF.
Measures by competent administrative authorities	<ul style="list-style-type: none"> Matters that business operators should note include appropriately performing customer identification by receiving principal identification documents, etc., and creating and saving verification records, etc. with guidance for improvement and correct, etc. given to business operators.

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

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> By using telephone forwarding services, customers can give their business a false appearance and can conceal the principal of ML/TF or ownership of criminal proceeds. Considering this, it is recognized that telephone forwarding services present the risk of being misused for ML/TF.
Measures by competent administrative authorities	<ul style="list-style-type: none"> Matters that business operators should note include sending transaction-related documents by registered mail that must not be forwarded or the like in non face-to-face transactions, checking corporate customers for beneficial owners of legal persons, checking the purposes of transactions, occupations of customers, etc., and creating and saving verification records. The competent administrative authorities have made improvements and corrections with respect to these matters by providing instructions ,etc. to business operators.

(16) Legal/Accounting Services Dealt with by Legal/Accounting Professionals

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> Legal/accounting professionals have high expertise in law and accounting, as well as high social credibility. Transactions through their services and related affairs can be a practical means of ML/TF. Actually, there are cases where services of legal/accounting professionals have been misused to disguise concealment of criminal proceeds as legitimate transactions. Considering this, it is recognized that when legal/accounting professionals conduct following transactions on behalf of clients, the services present a risk of misuse for ML/TF. <ul style="list-style-type: none"> ➤ Acts or procedures concerning buying and selling residential lots and buildings ➤ Acts or procedures concerning the establishment or merger of companies, etc. ➤ Management or disposal of cash, deposits, securities and other assets
Measures by competent administrative authorities, etc.	<ul style="list-style-type: none"> Competent administrative authorities and associations of each profession are also making efforts to promote AML/CFT measures, such as by developing regulations, preparing materials about duties, providing training, etc., and through such endeavors promote understanding of ML/TF risks among professionals.

5. High-Risk Transactions

- ✓ Referring to the FATF Guidance, measures under the Act on Prevention of Transfer of Criminal Proceeds, cleared cases of money-laundering offences, etc., high-risk transactions are identified from the viewpoints of “transaction types,” “countries/regions,” and “customer attributes,” and conduct analysis and assessment.
- ✓ The following is an overview of risk assessment and mitigation measures for each of the above viewpoints.

(1) Transaction Types and Risks

Forms	Assessment and Analysis Results	
Non-face-to-face Transactions	Assessment of Risks	<ul style="list-style-type: none"> • As non-face-to-face transactions may hinder business operators from directly seeing customers and identification documents, the accuracy of customer identification can be deteriorated. Therefore, compared with face-to-face transactions, non-face-to-face transactions make it easier for offenders to maintain high anonymity, falsify customer identification data and pretend to be a fictitious or other person by falsifying identification documents, etc. • Actually, there are cases where non-face-to-face transactions have been misused for money laundering, including a case where bank accounts opened by pretending to be another person were misused. Considering this, it is recognized that non-face-to-face transactions present a high risk of being misused for ML/TF.
	Measures by business operators	<ul style="list-style-type: none"> • Risk mitigation measures such as monitoring transactions based on the IP address and login address when judging whether transactions are suspicious.
Cash Transactions	Assessment of Risks	<ul style="list-style-type: none"> • In general, cash transactions have high liquidity and anonymity. Therefore, cash transactions may hinder the tracing of criminal proceeds unless business operators dealing with cash properly prepare transaction records. • In fact, there have been many cases where money launderers misused cash transactions by pretending to be other people. Considering this, it is recognized that cash transactions have carry a high risk of being misused for ML/TF.
	Measures by business operators	<ul style="list-style-type: none"> • Risk mitigation measures, such as refusing to conduct overseas remittances using cash brought in to the premises by a customer whose identity has not been verified because he/she does not hold an account, etc.
International Transactions	Assessment of Risks	<ul style="list-style-type: none"> • Compared with domestic transactions, international transactions can make it difficult to track ML/TF because domestic legislation and transaction systems, etc. vary from country to country. • In fact, in some cases, money laundering has been conducted through international transactions. Therefore, it is recognized that international transactions pose a risk for being misused in ML/TF.
	Measures by business operators	<ul style="list-style-type: none"> • Risk mitigation measures include visiting, etc., companies with which they plan to start foreign-exchange transactions to survey the details of their business, and refusing requests for overseas remittances that involve carrying cash across national borders.

5. High-Risk Transactions

(2) Countries/Regions and Risks

Assessment and Analysis Results

<p>Assessment of risks</p>	<ul style="list-style-type: none"> Based on the FATF public statements, we understand that transactions related to Iran or North Korea pose very high risks of misuse for ML/TF. In addition, the FATF published the names of countries/regions that have serious strategic deficiencies related to AML/CFT measures and have developed action plans to deal with them as countries/regions that continue to improve compliance with international AML/CFT measures. The FATF is calling on those countries/regions to promptly put those plans into action within the proposed periods of time. Transactions conducted with those countries/regions before the deficiencies pointed out by FATF are resolved are recognized to be risky.
<p>Measures to Mitigate Risks</p>	<ul style="list-style-type: none"> The Act on Prevention of Transfer of Criminal Proceeds and the Order stipulate that Iran and North Korea are jurisdictions deemed to have inadequate AML/CFT systems (hereinafter referred to as "specified jurisdictions"), and require that specified business operators must, upon conducting a specified transaction with a person who resides or is located in a specified jurisdiction and any other specified transactions that involve transfer of property to a person who resides or is located in a specified jurisdiction, conduct strict checks of the source of wealth and source of funds as well as customer identification data, etc.

(3) Customer Attributes and Risks (i)

Attributes Assessment and Analysis Results

<p>Anti-social forces (Boryokudan, etc.)</p>	<p>Assessment of Risks</p>	<ul style="list-style-type: none"> Other than committing various crimes to gain profit, Boryokudan and other anti-social forces conduct fundraising activities by disguising them as or misusing business operations. As money laundering obscures the source of funds from criminal activities or fundraising activities, money laundering is indispensable for anti-social forces. Thus, transactions with anti-social forces are considered to present high risk.
	<p>Measures by business operators</p>	<ul style="list-style-type: none"> Guidelines for How Companies Prevent Damage from Anti-Social Forces have been formulated to help companies, including companies other than specified business operators, to cut any relationships with anti-social forces they might have. Deposit-taking institutions, etc. are introducing clauses to exclude Boryokudan, etc. into their transaction terms and conditions. This is part of the effort to dissolve business relationships in case a customer has turned out to be Boryokudan, etc. If a customer has turned out to be a member of anti-social forces, financial institutions, etc. shall consider preparing STRs under the Act on Prevention of Transfer of Criminal Proceeds as a general business practice.

(3) Customer Attributes and Risks (ii)

Attributes	Assessment and Analysis Results
International terrorists (Such as Islamic Extremists)	<p>Assessment of risks</p> <ul style="list-style-type: none"> • Japan has been implementing the United Nations Security Council resolutions to freeze the assets of or implement measures against persons who are related to Al Qaeda or other terrorist groups. No person of Japanese nationality or residency has been included in this list, and there have been no terrorist acts carried out in Japan by terrorists identified by the United Nations Security Council so far. • However, the FATF pointed out in its report released in 2019 that even when there have not been any cases of terrorist attacks or terrorist financing in a country, that fact does not immediately lead to the conclusion that the risk of terrorist financing is low; the possibility of funds being collected in that country or being remitted overseas should not be excluded. • In light of the matters related to the threat of terrorism to Japan and the threat of and vulnerability to terrorist financing that have been pointed out internationally, the following activities should be recognized as concerns : <ul style="list-style-type: none"> ➤ Members of Islamic extremist and other terrorist groups hide themselves in communities of people from Islamic countries and misuse the communities for fundraising ➤ Terrorist financing may be provided through transactions disguised as legitimate ones conducted by Japanese organizations and companies <p>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.</p>
	<p>Measures to Mitigate Risks</p> <ul style="list-style-type: none"> • Necessary rules have been set up in the Act on Prevention of Transfer of Criminal Proceeds, Act on Punishment of Organized Crimes and Control of Crime Proceeds, Act on Punishment of Terrorist Financing, Foreign Exchange Act, and International Terrorist Asset-Freezing Act. • The Strategy to Make Japan “the Safest Country in the World” and the Counter Terrorism Guidance toward the Tokyo 2020 Olympic and Paralympic Games have been developed, and relevant ministries and agencies have been working on AML/CFT measures based on these decisions made by the government. • The police have been promoting anti-terrorist measures from the standpoints of both prevention and response to emergencies: <ul style="list-style-type: none"> ➤ Information collection and analysis, and thorough investigation ➤ Enhanced border security in collaboration with related agencies such as the Immigration Services Agency of Japan and Customs ➤ Promotion of anti-terrorist cooperation between government and private entities and protection of critical public facilities

(3) Customer Attributes and Risks (iii)

Attributes	Assessment and Analysis Results	
Non-resident Customers	Assessment of Risks	<ul style="list-style-type: none"> Because transactions with non-resident customers are not conducted face to face, non-residents can maintain a high level of anonymity, and it is easy for them to falsify customer identification data or to pretend to be a fictitious or other person. At the same time, business operators have limited means to conduct ongoing CDD compared with customers residing in Japan. Considering this, it is recognized that transactions with non-resident customers present a high risk in terms of ML/TF.
	Measures to Mitigate Risks	<ul style="list-style-type: none"> The Financial Services Agency's Guidelines for Supervision require business operators to develop internal control systems for suitable examination and judgment in order to file STRs. Such controls include detailed consideration of customer types and the circumstances behind transactions.
Foreign Politically Exposed Persons	Assessment of Risks	<ul style="list-style-type: none"> Foreign PEPs have positions and influence that can be misused for ML/TF. Grasp of their identification data, etc. is limited, and efforts to introduce anti-corruption measures vary from jurisdiction to jurisdiction. Depending on the situation, we recognize that transactions with foreign PEPs may carry a high risk of ML/TF.
	Measures to Mitigate Risks	<ul style="list-style-type: none"> When specified business operators conduct specified transactions with (1) the head of state of another country or a person who holds or used to hold an important position in a foreign government, etc., (2) any family member of (1), or (3) a legal person whose beneficial owner is either (1) or (2), the Act on Prevention of Transfer of Criminal Proceeds and its Order and Ordinance require that the business operators conduct enhanced CDD, including verifying the source of wealth and source of funds as well as customer identification data, etc.
Legal Persons without Transparency of Beneficial Ownership	Assessment of Risks	<ul style="list-style-type: none"> It is easy to conceal the identity of a natural person who has substantial owner of property by placing that property in the complex rights/control structures of legal persons. Such characteristics of legal persons make it difficult to track funds owned by legal persons and obscure beneficial owner. There are examples of cases where a bank account, which was opened in the name of a legal person without transparent beneficial ownership, was misused to conceal criminal proceeds derived from fraud and other crimes. Considering this, it is recognized that transactions with legal persons that do not have transparent beneficial owner present a high risk for ML/TF.
	Measures to Mitigate Risks	<ul style="list-style-type: none"> Japan has so far established systems under the Act on Prevention of Transfer of Criminal Proceeds, Ordinance for Enforcement of the Notary Act, Companies Act, etc. as systems to verify information on beneficial owners of legal persons. Also from the perspective of verifying information on the beneficial owner at the time of establishing a company, declaration of a person who is a beneficial owner, etc. requires a public notary.