

Tentative Translation

National Risk Assessment- Follow-up Report(2020)

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 November 2020. 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	– 6
4. Risk of Products and Services	7	– 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 3. Analysis of Money-Laundering Cases, etc.," "Section 4. Risk of Products and Services," and "Section 5. 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	Environment Surrounding Japan	—	Geographic Environment, Social Environment, Economic Environment, Criminal Circumstances, etc.
Section 3	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 4	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 5	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 6	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)

✓ 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, blackmailing, illicit drugs, and prostitution offenses.
Specialized Fraud Group	<ul style="list-style-type: none"> • Japan has recently witnessed a rise in specialized fraud cases. Damage in 2019 was concentrated in metropolitan areas. Tokyo (3,815 cases) accounted for 22.6% of the total number of cases recognized, and five prefectures, including Kanagawa (2,793 cases), Saitama (1,459 cases), Chiba (1,409 cases), and Osaka (1,809 cases), accounted for 67.0% of the total number of cases recognized. • 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 by skillfully abusing various means, including deposit and savings accounts, mobile phones, and call forwarding services. In this way, they commit organized fraud. In addition, they launder money, for example, by using bank accounts in the name of fictitious or other parties as a means to receive money from a victim. Furthermore, crime bases have spread to rental condominiums, rental offices, hotels, vehicles, etc., and the existence of foreign crime bases has surfaced. • 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 in which foreigners are involved are difficult to trace because they are transferred across borders between countries of different legal and transaction systems. Such crimes have characteristics that their human networks, manner of offenses, etc. are not limited within one country as seen in cases where crime groups consisting of foreigners in Japan, etc. commit crimes following instructions from criminal groups existing in their home countries, and these offenses tend to be more sophisticated and hidden as the roles of offenders are divided across borders.. • Vietnam and China lead the rankings of numbers of cleared offenses and account for more than 80% of the total for illegal transfers, etc. of deposit books, cash cards, etc. in violation of the Act on Prevention of Transfer of Criminal Proceeds in the last three years. • In terms of cleared cases for crime infrastructure related offenses, forgery of passports, residence cards, etc., are used to disguise residence status that allows work. It has been on an increasing trend since 2016.

3. Analysis of Money-Laundering Cases, etc. (Predicate Offenses): 1/4

- ✓ 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 2019 was about 63.3 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 2019 was about 46.9 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): 2/4

Predicate Offenses	Assessment and Analysis Results	
<p>Computer fraud</p>	<p>Forms of offenses</p>	<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. • The financial damage in 2019 consisted of 1,872 cases, and the amount was approximately 2.521 billion yen. The number of cases in 2019 was the second highest after 2014. In 2014, the number of cases hit the highest ever. The amount of financial damage in 2019 increased significantly compared to the previous year. • While Boryokudan involvement is observed in specialized fraud offenses, international criminal organizations have also been observed engaging in illegal remittance offenses related to Internet banking. The reality of the situation is that criminal organizations commit such offenses in an organized manner to obtain large amounts of criminal proceeds.
	<p>Modus operandi of money laundering</p>	<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 illegally remitted to accounts managed by the criminals from the accounts of the victims. 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. Furthermore, there were cases where crypto-assets obtained by fraudulent acts on the server of a crypto-asset wallet service were transferred to the anonymous account of a decentralized crypto-asset exchange managed by the criminal.
<p>Violation of the Investment Act/ Money Lending Business Act</p>	<p>Forms of offenses</p>	<ul style="list-style-type: none"> • This is a form of loan-shark crime whereby a money lending business operates without a registration and lends at a high interest rate. Cases include instances of lending without the lender and borrower directly meeting, where the borrower returns money by transferring it to an account in the name of another party. Lenders may send direct mail based on lists of heavy debtors • Large amounts of criminal proceeds are generated, and in 2019, the amount of damages reached over 6.7 billion yen, according to the statistics on cleared loan-shark crimes.
	<p>Modus operandi of money laundering</p>	<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.

<p>Predicate Offenses</p>	<p>Assessment and Analysis Results</p>	
<p>Habitual gambling/ Running a gambling place for profit</p>	<p>Forms of offenses</p>	<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.
	<p>Modus operandi of money laundering</p>	<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.
<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.

Predicate Offenses	Assessment and Analysis Results	
<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 60% of all narcotics-related crimes, the amount of stimulants confiscated in 2019 was the amount seized was 2,293.1 kg, a significant increase from the previous year and the highest ever. It exceeded 1,000 kilograms for 4 consecutive years from 2016 to 2019, and it can be assumed that smuggling and illicit trafficking of stimulants generates a large amount of criminal proceeds. Boryokudan gangsters, etc. accounted for at least 40% of the offenders in cleared cases of stimulant-related crimes during 2019. The situation of Boryokudan involvement continues. Evidence gathered in recent years strongly suggests that Boryokudan collude with overseas drug-related criminal organizations, and have been deepening their involvement in the distribution of stimulants . As of the offshore transaction of stimulant smuggling offenses, in 2019, Boryokudan gangsters and Taiwanese were cleared in the case of seizing about 587 kg.
	<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: 1/9

- ✓ 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. There are cases where financial products and services have been misused to receive or conceal criminal proceeds. As such, it is recognized that products and services of deposit-taking institutions present risks of misuse for money laundering. 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 under anonymous or fictitious names, borrowed names, and false names (including suspected ones) • Transactions where sudden large deposits and withdrawals are made despite accounts that normally do not move funds • Transactions, including remittances, deposits, and withdrawals performed in an unnatural manner and frequency in light of the purpose of the account holders' transactions, occupations, business contents, etc.
Measures by business operators	<ul style="list-style-type: none"> • Cases of a customer who was reported with STRs in the past, where an information-sharing system is established and when dealing with the customer. Details are confirmed by checking the documents and interviewing and then transaction is approved by the senior manager. • Cases where customer categories to be aware of when opening accounts are set. If a customer falls under a category, additional questions will be asked to confirm the rationality of opening the account. Additionally, if it is difficult to judge the rationality, the decision to open an account is made after the senior administrator's confirmation. • Cases of non-face-to-face transactions, where transaction monitoring is conducted focusing on access information, such as IP addresses and browser languages, with consideration of the possibility of spoofing.

4. Risk of Products and Services: 2/9

(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 under anonymous or fictitious names, borrowed names, and false names (including suspected ones). If an insurance premium is paid at the time of concluding a contract and then the contract is canceled promptly.
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 under anonymous or fictitious names, borrowed names, and false names (including suspected ones).
Measures by business operators	<ul style="list-style-type: none"> The confirmation and management of foreign customers' period of stay, the confirmation of the beneficial owners of legal persons using a third-party information agency, and freezing and transaction suspension of non-operating accounts as an example of enhanced customer due diligence. An example of transaction monitoring is promoted by adding deposit and withdrawal monitoring scenarios and grasping overseas transactions by detecting IP addresses.

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

(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. There are cases where a loan fraud is carried out under a fictitious name and fraudulent money is deposited into a fictitious name account that has been opened in advance.
Transactions that increase risk	<ul style="list-style-type: none"> Transactions under anonymous or fictitious names, borrowed names, and false names (including suspected ones).
Measures by industry association	<ul style="list-style-type: none"> Cases of checking phone numbers noticed by customers with a business operator's database to ascertain that the customers' telephone numbers are unique. Cases of detecting suspicious and unnatural transactions by utilizing IT vendors' systems and grasping when the telephone numbers notified by the customers were used.

(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 under anonymous or fictitious, borrowed names, and false names (including suspected ones) • Transactions having unnatural characteristics or conducted at an unnatural frequency considering the purpose of the transactions, occupation or business of the client, etc. • Frequent remittance transactions from a large number of persons
Measures by business operators	<ul style="list-style-type: none"> • Cases where risk is evaluated for each customer by taking into account the customer attributes and transaction conditions, and measures are taken according to the assessment • Cases of identifying and evaluating risks for services provided by a business operator acting as issuers of cards using the pre-paid payment methods when fund transfer services operate an issuer of that as a side business • Cases where upper limits are set for transaction amounts according to the product/service, transaction type, country/region, or customer attributes, and transactions exceeding those amounts are severely scrutinized (for example, upper limits for transaction amounts vary depending on visa status, such as permanent resident, technical intern, student studying abroad, etc.) • Cases where a resident card is presented as the principle identification document to confirm the period of stay and its period is controlled by using system when conducting a transaction with a foreigner

4. Risk of Products and Services: 5/9

(7) Crypto-assets Dealt with by Crypto-assets Exchange Service Providers

Item	Assessment and Analysis Results
Assessment of risks	<ul style="list-style-type: none"> • Important characteristics of crypto-assets are that its users are highly anonymous and that the transfer of crypto-assets can be quickly executed across national borders. In addition, regulation of crypto-assets differs from country to country. In light of these factors, if crypto-assets is misused for crimes, it becomes difficult to trace the proceeds derived from the crimes. • Considering actual cases where the anonymity of crypto-assets was misused to convert illegally obtained crypto-assets into cash through a crypto-assets exchange service provider and have the money remitted to an account opened in another person's name, it is recognized that crypto-assets is at risk of being misused for ML/TF. • And, considering that crypto-assets transactions are increasing globally and the environment surrounding such transactions is rapidly changing, it is recognized that the level of risk for misuse of crypto-assets for ML/TF, is relatively high in comparison to other types of business. Furthermore, since the deposit-taking institutions are strengthening their AML/CTF countermeasures, there are concerns that persons attempting to conduct ML/TF will use crypto-assets transactions in lieu of goods and services handled by the deposit-taking institutions. This situation is increasing the degree of risk associated with crypto-assets. • It is not easy to take appropriate and timely risk-mitigating measures amid rapid changes in the environment surrounding crypto-assets transactions, and if such efforts are insufficient, appropriate mitigating measures cannot be taken and the degree of risk will remain high.
Transactions that increase risk	<ul style="list-style-type: none"> • Transactions under anonymous or fictitious names, borrowed names, and false names (including suspected ones).
Measures by business operators	<ul style="list-style-type: none"> • Cases where as of the risk of using services in process of specialized fraud, the results of investigation and analysis related to the unnatural matching of customers' characteristics, such as their photos on identity verification documents and customer attributes found in the verification at the time of transactions, are reflected in documents prepared by specified business operators and verification at the time of transactions is strengthened. • Cases of strengthening the monitoring of transactions with countries judged to be highly risky and customers in the same countries by focusing on prosecution cases and media reports on financial crime-related remittances, risk analyses and the corruption perception indexes (CPIs) conducted by other countries' authorities. • Cases where the period of stay of foreign customers, such as international students and workers, is managed by a system after confirming it to deal with risks such as the sale of accounts at the time of their return to their home countries.

4. Risk of Products and Services: 6/9

(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 under anonymous or fictitious names, borrowed names, and false names (including suspected ones) Frequent transactions in a short period, etc.
Measures by business operators	<ul style="list-style-type: none"> Cases where principal identification documents, are required to be submitted even for transactions with an amount lower than the threshold value of the law, for which collation is conducted with those who are subject to economic sanctions and foreign PEPs. Cases where continuous transactions are monitored with a built-in camera (taken with each transaction), in addition to setting a fixed amount of transaction limit per transaction in foreign currency with automatic change machine.

(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 under anonymous or fictitious names, borrowed names, and false names (including suspected ones) Transactions related to financial leasing in which it is suspected of defrauding a financial leasing operator out of money under multiple financial leasing contracts, etc.
Measures by industry association	<ul style="list-style-type: none"> Respective business operators also establish basic policies and response manuals for AML/CFT measures, and establish specialized departments to deal with risks, including ML/TF risks. To prevent transactions that the lessee and the seller collude with each other without actual conditions, in addition to verification at the time of transactions in times of transaction, efforts are made, including the confirmation of the existence of substantial transactions for high-value transactions, new contracts, and leased properties with many accidents.

4. Risk of Products and Services: 7/9

(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"> Transactions under anonymous or fictitious names, borrowed names, and false names (including suspected ones) Credit card contracts in which it is suspected that the customer uses a fictitious or other person's name
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 under anonymous or fictitious names, borrowed names, and false names (including suspected ones)
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

4. Risk of Products and Services: 8/9

(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"> Transactions under anonymous or fictitious names, borrowed names, and false names (including suspected ones) The same person/company buying and selling a large amount of precious metals in a short period, etc.

(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 under anonymous or fictitious, borrowed names, and false names (including suspected ones) Transactions in which it is suspected that customers might use the service to disguise the company's actual status, etc.
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

4. Risk of Products and Services: 9/9

(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.

(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.
Transactions that increase risk	<ul style="list-style-type: none"> Transactions under anonymous or fictitious names, borrowed names, and false names (including suspected ones)

(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
Transactions that increase risk	<ul style="list-style-type: none"> Transactions under anonymous or fictitious names, borrowed names, and false names (including suspected ones)

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"> • For cash deposits and withdrawals that exceed a certain level, a hearing sheet is issued at the teller, and STRs are submitted if necessary, 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"> • Strengthening verification at the time of transaction for overseas remittance for areas close to countries and regions for which countermeasures were requested from member countries in the FATF statement. • Submitting by focusing on the discrepancy between the purpose of remittances from foreign countries and the recipients' actual usage of funds.

5. High-Risk Transactions

(2) Countries/Regions and Risks

Assessment and Analysis Results	
Assessment of risks	<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.

(3) Customer Attributes and Risks (i)

Attributes	Assessment and Analysis Results	
Anti-social forces (Boryokudan, etc.)	Assessment of Risks	<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.
	Measures by business operators	<ul style="list-style-type: none"> Some business operators regularly screen their customers using domestic and overseas databases at the start of transactions even after the start of transactions. In the case of customers falling under antisocial forces, such as Boryokudan and quasi-Boryokudan, STRs are reported.

5. High-Risk Transactions

(3) Customer Attributes and Risks (ii)

Attributes	Assessment and Analysis Results	
International terrorists (Such as Islamic Extremists)	Assessment of risks	<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 ➤ Foreign fighters engage in fundraising and other activities ➤ Persons who travel to conflict areas may become the parties conducting terrorist financing ➤ Terrorist financing may be provided through transactions disguised as legitimate ones conducted by Japanese organizations and companies ➤ Products and services provided by businesses can be abused in a way that avoids monitoring by business operators <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>

5. High-Risk Transactions

(3) Customer Attributes and Risks (iii)

Attributes	Assessment and Analysis Results	
Non-resident Customers	Assessment of Risks	<ul style="list-style-type: none"> In the case of transactions with non-resident customers, business operators have limited measures to conduct ongoing CDD compared with customers residing in Japan. Furthermore, when non-face-to-face transactions are conducted, anonymity will increase, and it is more difficult to track funds if ML/TF or the like is performed. Therefore, it is recognized that transactions with non-resident customers present a high risk in terms of ML/TF.
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.
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.