

National Risk Assessment- Follow-up Report(2022)

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 specified 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, specified 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 2022. For more details, refer to the full version of the NRA-FUR.

Table of Contents

1. Table of contents of the NRA-FUR	①
2. Environment surrounding Japan	②
3. Analysis of Money-Laundering Cases, etc. (Offenders, Modus Operandi, Suspicious Transaction Report)	③ ~ ⑧
4. Risk of Transaction Types, Country/Regions, and Customer Attributes	⑨ ~ ⑫
5. Risk of Products and Services	⑬ ~ ⑰

1 . Table of contents of the NRA-FUR

	Item		Main Description
	Introduction	History, Purpose, Overview of NRA-FUR	History of NRA-FUR preparation and publication, Purpose of NRA-FUR, and Overview of assessment and analysis result
Sec. 1	Risk Assessment Method, etc.	FATF Guidance, National Risk Assessment of Japan	Risk factor, Assessment process, Information used in the assessment
Sec. 2	Environment surrounding Japan	Geographic Environment	An island country located in a region called Northeast Asia (or East Asia)
		Social Environment	Population decline and Progress of aging, The numbers of foreigners entering Japan, etc.
		Economic Environment	The third largest economy in the world, One of the world's leading international financial centers
		Criminal Circumstances	Increase in cybercrime, Continuation of terrorism threats
Sec. 3	Analysis of Money Laundering Cases, etc.	Offenders	Boryokudan, Fraud(phone scam) Groups, and Crime groups of foreigners in Japan
		Modus Operandi	Crime forms of predicate offences (Theft, Fraud, and Narcotics-related crimes, etc.) and modus operandi of money laundering
		Suspicious Transaction Report	Number of Received STRs by Each Business Type, Number of STRs Used for Investigative Purposes, etc.
Sec. 4	Risk of Transaction Types, Country/Regions, and Customer Attributes	Transaction Types	Non-Face-to-face Transactions, Cash Transactions, and International Transactions
		Countries/Regions	Iran and North Korea
		Customer Attributes	Anti-social Forces, International Terrorists, Non-resident Customers, Foreign Politically Exposed Persons, and Legal Persons
Sec. 5	Risk of Products and Services	Major Products and Services in which Risk is Recognized	Products and Services Dealt with by specified business operators, etc. (Deposit-taking Institutions, Funds Transfer Service Providers, and Crypto-assets Exchange Service Providers, etc.)
Sec. 6	Low-risk Transactions	Factors that Mitigate Risks Types of Low-risk transactions	Specific transactions that have factors (The source of funds is clear, The customer is a national or local government, etc.) to mitigate risks
	Going Forward	—	Going forward of the competent authorizes and pecified business operators

2. Environment surrounding Japan

②

- ✓ The following is an overview of the environment surrounding Japan from the viewpoints of geographical environment, social environment, economic environment and criminal circumstances.

Assessment and Analysis Results

Geographic Environment

- Japan is an island country located in the eastern part of the Eurasian Continent, in a region called Northeast Asia (or East Asia). Traffic and logistics to and from other countries are conducted via the sea and airports. At seas and airports nationwide, immigration control and customs procedures are conducted from the viewpoints of preventing terrorism and smuggling committed by international criminal groups.

Social Environment

- The total population of Japan as of October 1, 2021 was approximately 125,500,000, making 11 consecutive years of decrease. The ratio of the population aged 65 and over to the total population reached a record high of 28.9%, which is higher than other developed countries.
- The number of foreigners entering Japan in 2021 was approximately 350,000, 91.8% less than in the previous year. This is a significant decrease since February 2020, when the government's measures against the COVID-19 pandemic began.
- The number of foreign residents as of the end of 2021 was approximately 2,760,000, 4.4% less than the previous year. In terms of the number of foreign residents by nationality and region, Chinese was the largest and accounted for 26.0% of the total, followed by Vietnamese and Koreans.

Economic Environment

- The Japanese economy occupies a vital position in the world economy. The third-largest economy after the United States and China. Besides, Japan has a highly developed financial sector as a global financial center. A considerable amount of financial transactions is conducted as one of the world's leading international financial centers.

Criminal Circumstances

- The total number of recognized criminal offense cases in 2021 continues to be a record low after the war as in the previous year. The number of elderly victims to the number of recognized criminal offenses has consistently increased.
- The number of ransomware attack cases reported to the NPA in 2021 was 146 cases, which has been increasing since the previous year, and the attacks affected all kind of companies and organizations, regardless of the size and industry type.
- The number of cleared cases of cybercrime was the highest ever in 2021. Cyberattacks conducted to steal information occur frequently, and the number of accesses considered to be search activities in cyberspace detected by the National Police Agency is also increasing. Thus, the threat in cyberspace has become a serious issue in Japan.
- As for international terrorist situation, terrorist attacks have occurred one after another in various parts of the world. There have also been cases in which Japanese people and interests of Japan related facilities have been targeted overseas by terrorism. Therefore, the threat of terrorism against Japan still exists.

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

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

Offenders	Assessment and Analysis Results
Boryokudan	<ul style="list-style-type: none">• Boryokudan repeatedly and continuously commit crimes to gain economic profit, and skillfully engage in money laundering with the gained criminal proceeds. In Japan, money laundering by Boryokudan is an especially serious threat.
Fraud (phone scam) Group	<ul style="list-style-type: none">• In recent years, the number of recognized fraud(phone scam) cases and the amount of loss suffered have remained high. The victims in 2021 were concentrated in metropolitan areas. The victims during 2021(14,498 recognized cases, and the total victim is about 28.2 billion yen) were geographically concentrated in the metropolitan areas, accounting for 70.6% of the total number of recognized cases in seven prefectures: Tokyo, Osaka, Kanagawa, Chiba, Saitama, Aichi, and Hyogo.• Having the ringleader as the core, fraud (phone scam) groups assign a role to each member. For example, one-member cheats victims, another withdraws money, and the other procures tools to commit the crime by skillfully abusing various means, including deposit and savings accounts, mobile phones, and call forwarding services. In this way, they commit organized fraud. In addition, they launder money, for example, by using bank accounts in the name of fictitious or third parties as a means to receive money from a victim.• There are some people who make bank accounts in the name of fictitious or third parties by using falsified identifications and thoughtlessly sell their own bank account. 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 with different legal and transaction systems. Such crimes are characterized by the fact that their human networks, mode of committing offenses, etc., are not limited to one country. This is evident in cases where crime groups consisting of foreigners, etc., in Japan commit crimes following instructions from criminal groups existing in their home countries, and these offenses tend to be more sophisticated and hidden since the tasks assigned are carried out by different offenders in different countries involved.• Observations of the situation indicate that foreigners in Japan who are involved in organized crime commit money laundering as part of their criminal activities; there were money laundering cases associated with a group of Chinese stole goods by impersonating a card holder with an unlawfully obtained credit card information and forwarded the goods to an offender who disposed of the goods, etc., a case of shoplifting by a group of Vietnamese, and a case of international fraud by a group of Nigerians.

3. Analysis of Money-Laundering Cases, etc. (Modus Operandi): 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 and Modus operandi of money laundering.

Predicate Offenses	Assessment and Analysis Results	
Theft	Forms of offenses Criminal proceeds	<ul style="list-style-type: none"> As for theft, there are also cases committed continuously and repeatedly by crime organizations, including Boryokudan and crime groups of foreigners in Japan, that result in large amounts of criminal proceeds. The total financial damages from theft during 2021 was about 47.4 billion yen (about 15.5 billion yen for the total amount of damage in cash), generating a large amount of criminal proceeds.
	Money laundering cases	<ul style="list-style-type: none"> Cases of buying and keeping stolen cars knowing that they were stolen. Cases where an offender used a flea market app to sell stolen goods in another person's name and made buyers transfer payments to a bank account under another person's name. Cases where a large quantity of stolen gold ingots was sold to a gold trader in the name of a legal person operated by a friend of the offender. Cases where a group of Vietnamese, etc. sent stolen cosmetics and other goods to another offender who disposed of the goods, etc. by lying about the names of goods or name of the sender written on the shipping label.
Fraud	Forms of offenses Criminal proceeds	<ul style="list-style-type: none"> Fraud offenses, including specialized fraud (phone scam) offenses, have been repeatedly and continuously committed by domestic and foreign criminal groups. Large amounts of criminal proceeds were generated through the use of bank accounts under the name of fictitious persons or other parties and transactions by a corporation disguised to appear as legitimate. The total financial damages from fraud offenses in 2021 was about 76.3 billion yen.
	Money laundering cases	<ul style="list-style-type: none"> Cases where an offender misused accounts under the names of individuals sold to crime groups when foreigners left Japan as accounts for receiving money stolen through fraud (phone scam). Cases where an offender opened and misused business accounts under the names of fake companies established for receiving proceeds from fraud (phone scam) or fraud targeting public benefits. Cases where an offender opened and misused accounts under fictitious names to receive proceeds from fraud.

3. Analysis of Money-Laundering Cases, etc. (Modus Operandi): 2/4

Predicate Offenses	Assessment and Analysis Results	
Computer fraud	Forms of offenses Criminal proceeds	<ul style="list-style-type: none"> • Computer fraud includes illegal remittance offences in which offenders operate ATMs by using illegally obtained cash cards of others, or IDs and passwords for online banking to illegally access the service system managed by financial institutions to transfer money from accounts under the names of others to accounts managed by the offenders. • Losses due to online banking fraud in 2021 was approximately 820 million yen.
	Money laundering cases	<ul style="list-style-type: none"> • Cases where the maximum amount of cash was withdrawn from ATMs using cash cards obtained via fraud (phone scam) offenses, and the maximum amount for transfer was illegally remitted to accounts under the name of another person managed by the criminals from the accounts of the victims. • Cases where a criminal organization in China illegally accessed a system of a financial institution in Japan by using IDs and passwords for online banking, etc. belonging to others and transferred money to an account under another person's name managed by the offenders to allow a Chinese criminal group in Japan to withdraw cash from the account. • Cases where an offender illegally used an electronic money payment app that was installed in a smartphone illegally obtained by the offender and added electronic money by making transfers from the bank account linked to the account in the app by impersonating the owner of the smartphone.
Violation of the Investment Act/ Money Lending Business Act	Forms of offenses Criminal proceeds	<ul style="list-style-type: none"> • This is loan-shark crime whereby a money lending business operates without a registration and lends money 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 under the name of another party. Lenders may send direct mails based on the personal information described in lists of heavy debtors or solicit an unspecified large number of persons through online advertisements or phone calls. • Large amounts of criminal proceeds are generated, and in 2021, the amount of damages reached over 9.4 billion yen, according to the statistics on cleared loan-shark crimes.
	Money laundering cases	<ul style="list-style-type: none"> • Loan sharks required borrowers to send repayments to a post-office box opened under the name of another individual or a fictitious business operator. • Loans sharks made borrowers issue bills and/or checks when lending money to the borrowers, and if there was any delay in repayment, the loan sharks brought such bills and/or checks to a financial institution to transfer money to an account under the name of another person • Loan sharks made a borrower transfer repayments to another borrower's account and made the second borrower send all or part of the repayments to another borrower to lend money to the third borrower.

3. Analysis of Money-Laundering Cases, etc. (Modus Operandi): 3/4

Predicate Offenses	Assessment and Analysis Results	
Violation of the Immigration Control Act	Forms of offenses Criminal proceeds	<ul style="list-style-type: none"> There have been cases where a foreigner forges a residence card for the purpose of giving an appearance of legitimacy when entering Japan, passing for a legal resident or a person with a valid work permit, etc.; cases where a foreigner possesses, uses, provides, or receives a forged residence card; cases where an offender forces a foreigner who does not have a work permit to work or arranges illegal employment for such a foreigner. In particular, regarding the promotion of illegal employment, there are cases of human trafficking where an offender places foreigners under his/her control by taking away their passports, etc., and forcing them to work. In 2021, there was a case where approximately 58 million yen of bank deposit claims for compensation for temporary employment became subject to confiscation and non-penal confiscation due to violation of the Immigration Control Act, in which offenders made foreigners in Japan undertake illegal employment.
	Money laundering cases	<ul style="list-style-type: none"> Cases where an offender made purchasers of forged residence cards pay for the cards by transfer to an account under another person's name. Cases where an offender received compensation for introducing foreigners remaining in Japan after the expiration of their authorized period of stay to employers as rental income under fictitious residence lease agreements.
Habitual gambling/ Running a gambling place for profit	Forms of offenses Criminal proceeds	<ul style="list-style-type: none"> There are various forms of gambling offenses, such as online casino gambling, in addition to hanafuda gambling, baseball gambling, and game-machine gambling. The reality is that Boryokudan are deeply involved in such gambling offenses, either directly or indirectly, and gambling is an important source of funds for them. In 2021, the orders for confiscation were issued against about 55 million yen in cash, which was the proceeds from running a gambling venue for profit.
	Money laundering cases	<ul style="list-style-type: none"> Cases where a gambling offense was committed in an online casino in which money bet by customers had to be paid to an account opened under another person's name. Cases where an offender made persons engaging in baseball gambling, etc. transfer dividends to an account under the name of another person. Case where criminal proceeds obtained via gambling offenses were processed as legal business proceeds using an innocent certified public tax accountant.

3. Analysis of Money-Laundering Cases, etc. (Modus Operandi): 4/4

Predicate Offenses	Assessment and Analysis Results	
Violation of the Amusement Business Act/ Violation of the Anti-Prostitution Act	Forms of offenses Criminal proceeds	<ul style="list-style-type: none"> Boryokudan have been directly or indirectly involved in certain cases. Examples include association with operators of illegal adult-entertainment businesses or sex-related amusement. Criminal proceeds from amusement-related offenses are an important source of funds for them. There were cases where foreigners who were staying illegally in Japan worked in the adult-entertainment business, etc. and cases where offenders forced victims to engage in prostitution by using violence, intimidation, etc. In 2021, there was a case where bank deposit claims of approximately 11 million yen, which were the proceeds made in violation of the Amusement Business Act, became subject to order for confiscation.
	Money laundering cases	<ul style="list-style-type: none"> Cases where an offender made customers at an unlicensed restaurant offering entertainment service pay for meals with a credit card payment terminal installed at another restaurant owned by the offender to receive proceeds made at the unlicensed restaurant. Cases where a Boryokudan member received proceeds from prostitution through a bank account under the name of a family member.
Drug-related crimes	Forms of offenses Criminal proceeds	<ul style="list-style-type: none"> Evidence gathered in recent years strongly suggests that Boryokudan collude with overseas drug-related criminal organizations, and is becoming more involved in the distribution of stimulants. As for the offshore transaction of stimulant smuggling crimes, in 2019, Boryokudan gangsters and Taiwanese were arrested in a case where about 587 kg was seized. As for overseas drug-related criminal organizations, Chinese, Mexican and West-African drug-related criminal organizations still have a strong presence. Criminal proceeds from drug-related offences are an important source of funds not only for criminal organizations in Japan but also for those based overseas. The number of cases of temporary restraining order for confiscation before institution of prosecution prescribed by the Anti-Drug Special Provisions Law in 2021 was 24, and the sum of monetary claims subject to the orders was about 32.7 million yen. In addition to monetary claims, properties that became subject to temporary restraining order for confiscation before institution of prosecution prescribed by the Anti-Drug Special Provisions Law in the past included vehicles, land and buildings, etc., which indicates that criminal proceeds obtained in cash, etc. are transformed into another type of property.
	Money laundering cases	<ul style="list-style-type: none"> Cases where traffickers of stimulants had buyers make payments by transfer to a bank account under another person's name. Cases where an offender had buyers make payments by transfer to a bank account and withdrew cash at an ATM, knowing that the payments were criminal proceeds obtained from the trafficking of cannabis.

4. Analysis of Money-Laundering Cases, etc. (STRs)

- ✓ Looking at the number of STRs submitted in 2021 by business type, banks, etc. occupy the largest share, accounting for 77.7% (411,683), followed by money lending companies 6.7% (35,442) and credit card companies 6.6% (34,904).
- ✓ The number of STRs used for the investigation, etc. by the prefectural police in 2021 was 353,832.

【Number of Received STRs by Each Business Type】

Category	Year	2019	2020	2021
		Number of reports	Number of reports	Number of reports
Financial institutions, etc.		415,299	402,868	495,029
Deposit-taking institutions		366,973	342,226	411,683
Banks, etc.		344,523	319,812	390,981
Shinkin Banks, Credit Cooperative		19,487	19,793	18,461
Labour Banks		371	300	318
Norinchukin Banks, etc.		2,592	2,321	2,523
Insurance Companies		2,876	2,635	3,458
Financial Instruments Business Operators		17,116	17,933	19,718
Money Lenders		17,316	25,255	35,442
Fund Transfer Service Providers		3,913	6,040	10,499
Crypto-assets Exchange Service Providers		5,996	8,023	13,540
Commodity Derivatives Business Operators		256	320	388
Currency Exchange Operators		712	252	201
Electronic Monetary Claim Recording Institutions		4	5	7
Others		137	179	93
Financial Leasing Operators		270	123	163
Credit Card Operators		24,691	29,138	34,904
Real Estate Brokers		6	7	4
Dealers in Precious Metals and Stones		217	63	48
Postal Receiving Service Providers		4	2	0
Telephone Receiving Service Providers		0	0	0
Telephone Forwarding Service Providers		5	1	2
Total		440,492	432,202	530,150

【Number of STRs Used for Investigative Purposes, etc.】

	2019	2020	2021
Number of STRs used in investigation	307,786	325,643	353,832

Examples of cleared cases detected through STRs by the prefectural police

Information on suspicious transactions reported by specified business operators is utilized in the investigation of money laundering, predicate offenses, etc.

- ✓ Cases of Violating the Act on Punishment of Organized Crimes, etc.
- ✓ Fraud Cases
- ✓ Cases of Violation of the Investment Act and Violation of the Money Lending Business Act
- ✓ Case of Violation of the Immigration Control and Refugee Recognition Act
- ✓ Narcotics-related crimes
- ✓ Case of Violating the Banking Act (Underground Banking)
- ✓ Cases of Fraud and Violating the Act on Prevention of Transfer of Criminal Proceeds

Examples of cases in which investigative organizations, etc. other than the prefectural police utilized STRs

The National Public Safety Commission and National Police Agency collect, organize and analyze the STRs and provide investigative organizations, etc. other than the prefectural police* as well with those that are considered to be useful for investigating money laundering offences or their predicate offences to enable the organizations to use them for secret investigations, criminal investigations and investigations into tax offences, etc. Meaning the investigative organizations, etc. set forth in Article 13, paragraph 1 of the Act on Prevention of Transfer of Criminal Proceeds.

5. Risk of Transaction Types, Country/Regions, and Customer Attributes: 1/4

9

- ✓ Referring to the FATF Recommendations, cleared cases of money-laundering offences, etc., analysis and assessment of risks were conducted from the viewpoints of "transaction types," "countries/regions," and "customer attributes."
- ✓ The following is an overview of risk assessment for each of the above viewpoints.

(1) Transaction Types

Attributes		Description
Non-face-to-face Transactions	Assessment of Risks	<ul style="list-style-type: none"> • As non-face-to-face transactions may hinder specified 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 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.
	Money laundering cases Modus Operandi	<ul style="list-style-type: none"> • A criminal obtained criminal proceeds from benefits fraud related to COVID-19 by impersonating a different person through having the government transfer funds to a bank account, and sent the funds to a bank account under another person's name through an online non-face-to-face transaction. • A criminal sent criminal proceeds from fraud to an account for crypto-asset transactions through an online non-face-to-face transaction and purchased crypto-assets.
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.
	Money laundering cases Modus Operandi	<ul style="list-style-type: none"> • Cases where goods obtained by theft or fraud, etc. are converted into cash. • Cases where criminals receive criminal proceeds by transfer to a bank account under a fictitious or another person's name and convert them into cash at an ATM. • Cases where criminal organizations, etc. receive criminal proceeds in cash. • International money laundering cases where an international criminal organization withdrew a large amount of cash in a single transaction by disguising the legitimacy of transactions, in which criminal proceeds from fraud in a foreign country were sent to a financial institution in Japan. <p>In these cases, it is difficult to trace the movement of funds due to the existence of cash transactions, and it is recognized that the vulnerability of products and services provided by specified business operators, as well as the liquidity and anonymity, etc. of cash, are misused for ML/TF.</p>

(1) Transaction Types

Attributes		Description
International Transactions	Assessment of Risks	<ul style="list-style-type: none"> In transactions with foreign countries, it is difficult to trace transferred funds compared to domestic transactions because of the difference in legal systems and transaction systems. 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. Transactions related to countries and regions where proper AML/CFT measures are not implemented and International remittances originated from large amounts of cash, etc. are recognized as high risk.
	Money laundering cases Modus Operandi	<ul style="list-style-type: none"> The modus operandi used in the above cases include: <ul style="list-style-type: none"> ✓ To misuse financial institutions, etc. in and outside Japan (cross-border remittances, etc.); ✓ To disguise money laundering as legal trading (export or import of goods, etc.); ✓ To provide domestic and cross-border remittance and payment services without actually moving funds; and ✓ To use cash couriers. Specific characteristics of modus operandi used in money laundering cases, in which offenders try to hide the true source of funds or facts about funds by disguising criminal proceeds from fraud committed overseas as legitimate funds, include: <ul style="list-style-type: none"> ✓ A large amount of money, sometimes over 100 million yen, is remitted each time. ✓ The reasons for remittance given by the receiver and the remitter may be different. ✓ Almost all the remitted amount is withdrawn in cash. ✓ The remitters request reverse transactions later. In money laundering cases or underground banking cases disguised as legal trading, the following characteristics were found: <ul style="list-style-type: none"> ✓ To export goods with export permits obtained by preparing false documents; and ✓ To export goods in high demand outside Japan (such as cars and heavy machinery) and convert them into cash at export destinations as a way to make cross-border remittances. <p>In this way, the forms of criminal proceeds change from cash to goods and back to cash again.</p>

(2) Countries/Regions

Assessment of Risks

- We understand that transactions related to Iran or North Korea pose very high risks.
- The FATF published the names of countries/regions that have serious strategic deficiencies related to AML/CFT measures and have developed action plans to deal with them as countries/regions that continue to improve the 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. Therefore, transactions conducted with those countries/regions before the deficiencies pointed out by FATF are resolved are recognized to be risky.

(3) Customer Attributes^①

Attributes

Assessment of Risks

Anti-social Forces (Boryokudan, etc.)

- Other than committing various crimes to gain profit, Boryokudan and other anti-social forces conduct fundraising activities by disguising them as or misusing business operations. As money laundering makes the source of funds from criminal activities or fundraising activities unclear, money laundering is indispensable for anti-social forces. Since anti-social forces engage in money laundering, transactions with anti-social forces are considered to present high risk.

International terrorists (Such as Islamic Extremists)

- No person of Japanese nationality or residency has been included in the list of persons whom asset freezing measures are implemented against pursuant to the United Nations Security Council resolutions (No. 1267 and succeeding resolutions as well as No. 1373), and there have been no terrorist acts carried out in Japan by the terrorists designated 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 and 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:
 - Products and services provided by specified business operators can avoid their monitoring to be misused, etc.
 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.

(3) Customer Attributes②

Attributes	Assessment of Risks
Non-resident Customers	<ul style="list-style-type: none"> In the case of transactions with non-resident customers, specified business operators have limited measures to conduct ongoing CDD compared with customers residing in Japan. Furthermore, when non-face-to-face transactions are conducted or when identification documents issued by foreign governments, etc. are used, 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	<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, it is recognized that transactions with foreign PEPs present a high risk in terms of ML/TF.
Legal Persons without Transparency of Beneficial Ownership	<ul style="list-style-type: none"> Legal persons can make the rights and controlling interests in their properties complicated. Beneficial owners of legal persons can conceal the fact that they have substantial rights to such properties by making their properties belong to legal persons. Therefore, it is considered that there are risks in engaging in transactions with legal persons. Looking at the risks by form of legal person, existing stock companies are at a risk of abuse, considering that they are established through strict procedures, etc., hold a high degree of trust from the general public, and their shares can be easily transferred. On the other hand, newly established holding companies are at a risk of abuse, considering that they are generally established through simple procedures and can be maintained at low cost. There are examples of cases where a bank account, which was opened in the name of a legal person without transparent beneficial owner, was misused to conceal criminal proceeds derived from fraud and other crimes. Considering this, it is recognized that transactions with legal persons that do not have transparent beneficial owner present a high risk for ML/TF.

- ✓ 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.

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

Assessment of Risks

- Deposit-taking institutions provide various products and services, including accounts that guarantee safe fund management, deposit transactions for quick preparation or storage of funds regardless of time and place, exchange transactions for transferring funds from one place to another or to many people quickly and securely, safe-deposit boxes for safe storage of property while maintaining secrecy, and bills and checks that are negotiable and easy to transfer.
On the other hand, those same characteristics of financial products and services can make them convenient for transferring criminal proceeds. There are cases where financial products and services have been misused to receive or conceal criminal proceeds. As such, it is recognized that products and services of deposit-taking institutions present risks of misuse for money laundering.
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, figures in the statistics of transactions misused for ML/TF, 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.
- Most of the modus operandi used for cleared cases of concealment of criminal proceeds in 2020 involved money transfer to third-party accounts. There were more than a dozen accounts under the names of other people that had been misused in some past cases. Furthermore, hundreds of passbooks were seized from the crime base of a person arrested for soliciting the transfer of accounts. Accounts in other people' names are the main criminal infrastructure of ML/TF, among others. Deposit-taking institutions who provide the accounts must take continuous measures to prevent the transfer of accounts and subsequently detect illegal transactions.

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

Assessment of Risks

- Since insurance products with cash accumulation features enable criminal proceeds 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.

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

Assessment of Risks

- Financial instruments business operators and commodity derivatives business operators provide products and services for customers to conduct stock investment and commodity derivatives transactions, etc. Offenders planning to engage in ML/TF use such products and services to convert criminal proceeds to various rights, etc. and increase such obtained rights, etc. using criminal proceeds.
- Some financial instruments business operators manage funds contributed to investment funds. If funds from criminal proceeds are provided for investment funds with complex structures, it becomes difficult to trace the source of funds. Therefore, investment made through financial instruments business operators and commodity derivatives business operators can be an effective method for money laundering.
- Indeed, there are cases where criminal proceeds from fraud or embezzlement have been invested in stocks or commodity derivatives. Considering relevant situations, it is recognized that investment made through financial instruments business operators, etc. and commodity derivatives business operators may involve risks of misuse for ML/TF.

(4) Trust Dealt with by Trust Companies etc.

Assessment of Risks

- Trusts have the functions of transferring property rights from a settlor to a trustee, changing the nominee of the property when it is subject to a registration system, and altering the attribution, quantity and nature of the property. Furthermore, trusts can come into force on conclusion of a trust contract between parties involved or as self-settled trust. Because of such characteristics, offenders attempting ML/TF may be able to separate themselves from criminal proceeds and conceal the relationship with the proceeds if they misuse a trust.
- No cleared money laundering case involving misusing trusts has been reported in Japan in recent years. However, these characteristics mean that trusts can be considered as risky for misuse in ML/TF.

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

Assessment of Risks

- Money lending by money lenders, etc. can make tracking criminal proceeds difficult. Considering a relevant situation, it is recognized that money lending by money lenders, etc. carries the risk of misuse for ML/TF.
- There are cases where an offender carried out loan fraud by identifying himself as a fictitious person, etc. and deposited fraudulent money into an account under the fictitious name that has been opened in advance. There is a risk of misuse for generating criminal proceeds.

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

Assessment of Risks

- Funds transfer services can be a useful method for ML/TF, given the characteristics of funds transfer services in which foreign exchange transactions are performed as a business, as well as the existence of funds transfer service providers that offer services to remit to many countries and the existence of type I funds transfer services, which allow large amounts of foreign exchange transactions.
- 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 identification documents and pretending to be the person. There have also been cases where a malicious third party opened an account at a funds transfer service provider under the name of an account holder after obtaining the account information of the account holder illegally, linked the account with a bank account, and illegally withdrew money by depositing funds (recharging) from the bank account to an account at the funds transfer service provider. Considering these situations, it is recognized that funds transfer services present risks of misuse for ML/TF.
- In light of the fact that both the number of remittances per year and the amount handled per year by funds transfer service providers are increasing and the fact that there is an ongoing discussion as to whether the payment of wages to accounts at funds transfer service providers should be allowed or their participation in the *Zengin* system (all-bank data telecommunications system) should be allowed, we consider the degree of risk that funds transfer services present in terms of misuse for ML/TF to be growing compared to other business categories.

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

Assessment of Risks

- Crypto-assets allow users to be anonymous and enable instant cross-border transfers. In addition, some countries have no or inadequate regulation on crypto-assets. If crypto-assets exchange service providers in these countries are abused for crimes, it is difficult to trace the transfer of such crypto-assets.
- Indeed, there have been cases where offenders abused the anonymity of crypto-assets to change them into cash after moving them through overseas crypto-assets exchange service providers and deposit funds in an account in another person's name. For this reason, it is considered that crypto-assets are at risk of abuse 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. Although deposit-taking institutions have improved their AML/CFT measures, there are cases where persons who intend to commit ML/TF used crypto-asset transactions in addition to products and services handled by deposit-taking institutions by utilizing the fact that not all deposit-taking institutions have sufficient knowledge about crypto-asset transactions. This situation is increasing the degree of risk associated with crypto-assets.
- It is not easy to implement measures to lower the degree of risk timely and appropriately due to the rapid change in the environment surrounding crypto-assets transactions, so crypto-assets exchange service providers need to implement high-level measures in advance. If such measures are not taken sufficiently, crypto-assets exchange service providers will not be able to lower the degree of risk appropriately, and the degree of risk will remain high.

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

Assessment of Risks

- Foreign-currency exchange can be a part of a strategy to take the proceeds of crime abroad. Foreign-currency exchange is usually carried out in cash, which is highly liquid and can be possessed or transferred without information about the bearer. From these characteristics, foreign-currency exchange can be a useful way to launder money or finance terrorism.
- Actually, there has been a case where foreign currency obtained as criminal proceeds of crime committed overseas was converted to Japanese yen through a third party who did not know the actual circumstances. Considering this relevant situation, it is recognized that foreign-currency exchange carries risks of misuse for ML/TF.

(9) Financial Leasing Dealt with by Financial Leasing Operators

Assessment of Risks

- Although there were no cleared money laundering cases involving the misuse of financial leasing, because finance leases have the characteristic of a lessee and a seller being able to conspire to conduct a false transaction, it is considered that finance leases are at risk of being misused for ML/TF.

(10) Credit Cards Dealt with by Credit Card Operators

Assessment of Risks

- Credit cards allow a holder of criminal proceeds in cash to transform them into different kinds of property. It is also possible to transfer funds by providing a credit card to a third party and making him purchase products. Considering this, it is recognized that credit cards present the risk of misuse for ML/TF.

(11) Real Estate Dealt with by Real Estate Brokers

Assessment of Risks

- Real estate has high value and can be exchanged for large amounts of cash. Furthermore, it is possible for offenders to transfer criminal proceeds by, for example, paying more than the market value for a property. From these aspects, real estate can be a convenient instrument for ML/TF.
- Actually, there have been some cases where criminal proceeds from prostitution or fraud were used to buy real estate. Considering this, real estate presents a risk of misuse for ML/TF.
- Recently, there have been many cases where real estate was purchased for the purpose of preserving assets or investment, and there is a risk that crime organizations in and outside Japan, etc. have been misusing real estate transactions to change the form of criminal proceeds.

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

Assessment of Risks

- Precious stones and metals have high financial value, are easy to transport and exchanged with cash all over the world, and are highly anonymous because it is difficult to trace their distribution channel and location after transactions. In particular, since gold bullion are usually purchased with cash, they can be an effective method for ML/TF.
- 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.

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

Assessment of Risks

- Postal receiving services are misused to provide locations for sending proceeds derived from crime, such as fraud and sales of illegal goods. If falsified customer identification data is provided to conclude a service contract, it can be difficult to identify the party committing the ML/TF or ownership of the criminal proceeds. Therefore, postal receiving services can be an effective instrument for ML/TF.
- Actually, there are cases where offenders made contract with postal receiving service providers under fictitious names and deceived the providers into receiving criminal proceeds through concealment. Considering this, it is recognized that postal receiving services present a risk of misuse for ML/TF.

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

Assessment of Risks

- Recently we have not seen any cleared cases for money laundering involving misuse of a telephone receiving service providers. 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

Assessment of Risks

- By using telephone forwarding services, customers can give their business a false appearance and conceal the offenders committing ML/TF or the ownership of criminal proceeds. Thus, it is recognized that telephone forwarding services present a risk of being misused for ML/TF concealing the criminal proceeds obtained from specialized fraud (phone scam), etc.

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

Assessment of Risks

- Legal/accounting professionals have high expertise in law and accounting, as well as high social credibility. Transactions through their services and related affairs can be an effective means of ML/TF.
- Actually, there are cases where services of legal/accounting professionals have been misused to disguise concealment of criminal proceeds as legitimate transactions. Considering this, it is recognized that when legal/accounting professionals conduct following transactions on behalf of clients, the services present a risk of misuse for ML/TF.
 - Acts or procedures concerning buying and selling residential lots and buildings
 - Acts or procedures concerning the establishment or merger of companies, etc.
 - Management or disposal of cash, deposits, securities and other assets

- **JAFIC TOP PAGE**

<https://www.npa.go.jp/sosikihanzai/jafic/index.htm>

- ◆ **Annual Report and National Risk Assessment**

<https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/nenzihokoku.htm>

- ◆ **Reference cases of suspicious transactions**

<https://www.npa.go.jp/sosikihanzai/jafic/todoke/gyosei.htm>

- **THE WHITE PAPER**

https://www.npa.go.jp/publications/whitepaper/index_keisatsu.html

- **Statistics and other data held by the National Police Agency
(Fraud (phone scam), Organized Crime, Crime Statistics, etc.)**

<https://www.npa.go.jp/publications/statistics/index.html>