The Japanese version is the authoritative version,
and the English version is for reference only.

December 2023

National Risk Assessment-Follow-up Report

【 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 submit 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 2023. For more details, refer to the full version of the NRA-FUR.

Table of Contents

1． Overview of NRA-FUR 2023

Introduction（History, Purpose, Overview）

Section 1. Risk Assessment Method, etc.

Section 2. Environment Surrounding Japan

1. Geographic Environment 2. Social Environment 3. Economic Environment 4. Criminal Circumstance, etc.

Section 3． Analysis of Money Laundering Cases, etc.

Offenders	Modus Operandi	Suspicious Transaction Report
1. Boryokudan 2. Online and telephone fraud Group 3. Crime groups of foreigners in Japan	1. Predicate Offences（Theft, Fraud, etc.） 2. Major Transactions, etc. misused for ML	1. Reported number of STRs by business type

Section 4. Risk of Transaction Types, Countries/Regions, and Customer Attributes

Transaction Types	Countries/Regions	Customer Attributes
1. Non-Face-to-face Transactions 2. Cash Transactions 3. Cross-border Transactions	1. Countries/Regions against which the implementation of countermeasures are requested by the FATF Recommendations（particularly high-risk）Iran and North Korea 2. Countries/Regions subject to applying enhanced due diligence measures proportionate to the risks arising from the jurisdiction requested by the FATF Recommendations (high-risk) Myanmar, (Result of the June 2023 FATF Plenary)	1. Boryokudan, etc. 2. International terrorists（Islamic extremists, etc.） 3. Non-residents customers 4. Foreign politically exposed persons 5. Legal Persons (legal persons without transparency of beneficial owners, etc.)

Section 5. Risk of Products and Services

Transactions of relatively higher risk than other business forms	●Products and services dealt with by deposit-taking financial institutions ●Funds transfer services ●Crypto assets	Transactions that are expected to have a relatively higher risk compared to other business forms	●Electronic payment instruments
Transactions considered to be of risks	●Insurance ●Foreign currency exchange ●Precious metals/stones ●legal/Accounting services ●Investment ●Finance leasing ●Postal receiving services ●Trust ●Credit cards ●Telephone receiving services ●Money lending ●Real estate ●Telephone forwarding services		

Section 6. Low-risk Transactions（Transactions for which simplified CDD is permitted, prescribed in Article 4 of the Ordinance）

Going Forward

2．Table of contents and main description　1/4

②

,.	Item		Main description
	Introduction		○ History, Purpose, Overview ○ Overview of risk analysis ○ Major changes • **Overview of the FATF Recommendation Compliance Act**【NEW】
Sec.1	Risk Assessment Method	FATF Guidance NRA of Japan	○ Risk factors ○ Assessment process ○ Assessment method ○ Information used in the assessment
Sec.2	Environment Surrounding Japan	Geographic	○ Geographic environment （Location, national land area, etc.）
		Social	○ Social environment（Population, the number of foreigners entering japan, the number of foreign residents, etc.）
		Economic	○ Economic environment（Economic scale, financial scale, etc.） • **Annual number of notifications of STRs related to Main countries under Economic sanctions**【NEW】
		Criminal Circumstances, etc.	○ Criminal circumstance • Number of recognized criminal offence cases, etc. • Cyber crimes, etc.(Online banking fraud cases, ransomware, cyber-attack, status of cleared cases) ○ Terrorism situation
Sec.3	Analysis of ML Cases etc.	Offenders	○ Boryokudan ○ Online and telephone fraud Group • **Recent situation concerning crimes committed by online and telephone fraud group**【NEW】 ○ Crime groups of foreigners in Japan • Recent situation concerning crimes committed by foreigners in Japan

2. Table of contents and main description 2/4

		Item	Main description
Sec.3	Analysis of Money Laundering Cases, etc.	Offenders	○ Predicate offences（Theft, fraud, etc.） • **Money Laundering etc. related to Ransomware**【NEW】 ○ Major Transactions, etc. Misused for Money Laundering
		Modus Operandi	○ Annual Reported Number of STRs by Business Type • Examples of Cleared Cases Detected through STRs by the Prefectural Police • Examples of Cases in Which Investigative Organizations, etc. Other than the Prefectural Police Utilized STRs
Sec.4	Risk of Transaction Types, Countries/Regions, and Customer Attributes	Transaction Types	○ Non-Face-to-face Transactions ○ Cash Transactions ○ Cross-border Transactions } Revised risk mitigate measures
		Countries/Regions	○ Countries/Regions against which the implementation of countermeasures are requested by the FATF Recommendations **North Korea, Iran** ○ Countries/Regions subject to applying enhanced due diligence measures proportionate to the risks arising from the jurisdiction requested by the FATF Recommendations【NEW】 **Myanmar** ○ Countries and Regions with Suspended FATF Membership【NEW】 **Russia** 【At the time of the FATF Plenary at June 2023】
		Customer Attributes	○ Boryokudan, etc. ・・・Include “Anonymous and Fluid Crime Group” ○ International Terrorists (Such as Islamic Extremists) • **Risk of Abuse of Nonprofit Organizations for TF（REVISED）** ○ Non-resident Customers ○ Foreign Politically Exposed Persons ○ Legal Persons (Legal Persons without Transparency of Beneficial Owner, etc.)

2. Table of contents and main description 3/4

④

Item			Main description
Sec.5	Risk of Products and Services	Major Products and Services in which Risk is Recognized	○ Products and Services Dealt with by Deposit-taking Institution • **Electronic Payment Handling Services, etc.【NEW】** • **Emergency Countermeasures Plan for Robbery and Online and Telephone Fraud Cases Using the Method of Recruiting Perpetrators on Social Media【NEW】** ○ Insurance Dealt with by Insurance Companies, etc. ○ Products and Services, etc. Dealt with by Financial Instruments Business Operators, etc., and Commodity Derivatives Business Operators ○ Trust Dealt with by Trust Companies, etc. ○ Money Lending Dealt with by Money Lenders, etc. ○ Funds Transfer Services Dealt with by Funds Transfer Service Providers ○ **Electronic Payment Instruments Dealt with by Electronic Payment Instruments Service Providers【NEW】** ○ Crypto-assets Dealt with by Crypto-assets Exchange Service Providers • **International Trends in Crypto Assets, etc.（REVISED）** ○ Foreign Currency Exchanges Dealt with by Currency Exchange Operators ○ Financial Leasing Dealt with by Financial Leasing Operators ○ Credit Cards Dealt with by Credit Card Operators • Status of Consideration for Strengthening Security Measures in Credit Card Payment Systems【NEW】 ○ Real Estate Dealt with by Real Estate Brokers ○ Precious Metals and Stones Dealt with by Dealers in Precious Metals and Stones ○ Postal Receiving Services Dealt with by Postal Receiving Service Providers ○ Telephone Receiving Services Dealt with by Telephone Receiving Service Providers ○ Telephone Forwarding Services Dealt with by Telephone Forwarding Service Providers ○ Legal/Accounting Services Dealt with by Legal/Accounting Professionals **【High -Value Electronically Transferable Prepaid Payment Instruments Dealt with by Issuers】(REVISED)** 【Casino】

2. Table of contents and main description 4/4

⑤

Item			Main description
Sec.6	Low-risk Transactions	Factors that Mitigate Risks	○ Source of funds is identified ○ The customer, etc., is the national government or a local public entity ○ Customers, etc., are limited under laws and regulations. ○ The transaction process is supervised by the national government, etc. based on laws, etc. ○ It is difficult to disguise the actual status of legal persons, etc. ○ Minimal or no fund-accumulation features ○ The transaction amount is less than the regulatory threshold ○ Customer identification measures are secured by laws, etc.
		Types of Low-risk Transactions	○ Certain Transactions in Money Trusts, etc. ○ Conclusion, etc. of Insurance Contracts ○ Payment of Maturity Proceeds, etc. ○ Transactions Carried out in a Securities Market (exchange), etc. ○ Transactions of Government Bonds, etc., that are Settled by an Account Transfer at the Bank of Japan ○ Certain Transactions concerning the Loan of Money, etc. ○ Certain Transactions in Cash, etc. ○ Opening a Special Account under the Act on Book-Entry Transfer of Corporate Bonds and Shares ○ Transactions through SWIFT ○ Specified Transactions in Financial Leasing Contracts ○ Buying and Selling Precious Metals and Stones, etc., in Which the Payment is Made through Methods Other Than Cash ○ Certain Transactions with Telephone Receiving Services ○ Transactions with the National Government, etc., as a Customer ○ Specific Transactions in Agent Work, etc., for Specified Mandated Acts by Judicial Scriveners, etc.
	Going Forward	—	Going forward of the competent authorizes and specified business operators

3. Environment surrounding Japan

Assessment and Analysis results	
Geographic Environment	• Japan is an island country located in the eastern part of the Eurasian Continent. • 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 crime groups.
Social Environment	• The total population of Japan as of October 1, 2022, was approximately 124.95 million, marking 12 consecutive years of decrease. The ratio of the population aged 65 and over to the total population reached a record high of 29.0%, which is higher than in other developed countries. • The number of foreigners entering Japan in 2022 was approximately 4.2 million. Although this represents a significant increase from the previous year due to the relaxation of border control measures implemented to prevent the spread of COVID-19, it is still about 27 million (approximately 86.5%) less than the number of entrants before the pandemic in 2019. • The number of foreign residents as of the end of 2022 was approximately 3.08 million, 11.4% more than the previous year. In terms of the number of foreign residents by nationality and region, Chinese was the largest and accounted for 24.8% 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. • Japan has a highly developed financial sector as a global financial center. A considerable number of financial transactions are conducted as one of the world's leading international financial centers.
Crime Circumstance etc.	• The total number of recognized criminal offence cases has consistently decreased since 2003. However, in 2022, there were 601,331 cases, surpassing the post-war record low in 2021 (an increase of 5.8% compared to the previous year), indicating a situation that requires close attention for future trends. • In 2022, the situation surrounding cyber threats was extremely serious. This includes an increase in ransomware infection damages, the revelation of cyber-attacks targeting crypto-asset-related businesses and academic figures in Japan, and a sharp increase in online banking fraud cases in the latter half of the year. • Terrorist attacks occurred worldwide, and there were also cases in which Japanese people and the interests of Japan abroad were targeted by terrorism.

4. Analysis of Money Laundering Cases, etc.（Offenders） 1/3

The number of cleared Money Laundering cases * in 2022 was 726, an increase of 94 cases compared to the previous year.

Category \ Year	2020		2021		2022	
	Number of cases	Percentage (%)	Number of cases	Percentage (%)	Number of cases	Percentage (%)
Number of cleared cases of money laundering offences	600	—	632	—	726	—
Related to the Act on Punishment of Organized Crimes	597	99.5	623	98.6	709	97.7
Related to the Anti-Drug Special Provisions Act	3	0.5	9	1.4	17	2.3

Offenders	Assessment and Analysis results
Boryokudan	• In Japan, money laundering by Boryokudan is an especially serious threat. • In terms of the number of cleared cases of money laundering from 2020 to 2022 in which Boryokudan gangsters were involved in relation to predicate offences, the majority was fraud, theft, and loan sharking • Furthermore, the total amount of criminal proceeds (limited to those that can be monetized) was approximately 1.35 billion yen. As to the form of these criminal proceeds, cash including bank deposits, accounted for 75.8% of the cleared cases, with an average of about 7.3 million yen per case. • When analyzed by transaction type, domestic money transfers* accounted for 31.3% of all cases, while 21.6% of cases involved receiving criminal proceeds in cash without involving any goods or services. • Boryokudan repeatedly and continuously commit crimes to gain economic profit, and skillfully engage in money laundering with the gained criminal proceeds.

4. Analysis of Money Laundering Cases, etc.（Offenders） 2/3

Offenders	Assessment and Analysis results
Online and telephone fraud Group	• Fraud groups involved in Online and telephone fraud schemes orchestrated by the mastermind, have become more sophisticated by subdividing roles such as so-called “callers,” “receivers,” “senders,” “cash collectors & carriers,” “recruiters,” “crime tool procurement agents,” etc. They use highly secretive communication methods for instructions and coordination between the leaders and the executors. Furthermore, they cleverly misuse various tools, such as deposit/savings accounts, mobile phones, telephone-forwarding services, etc., to commit organized fraud. • There are some people who thoughtlessly sell their own bank accounts or bank accounts opened under the names of fictitious or third parties by using falsified identifications. • Malicious businesses that illegally transfer deposit/savings accounts and mobile phones to fraud groups or provide services like telephone forwarding still exist. **[Recent Situation concerning Crimes Committed by Online and Telephone Fraud Group]** • In 2022 , the number of recognized online and telephone fraud cases was 17,570, with the total damage amounting to 37.08 billion yen. These figures represent an increase compared to the previous year, and the amount of damage has increased for the first time in eight years, indicating a serious situation. • While the stolen money is often received in cash or deposited into bank accounts under the names of fictitious or other parties, there are also cases where electronic money rights (prepaid payment methods) are illegally obtained. • To avoid freezing by financial institutions after the discovery of the crime, the criminals tend to refund immediately, transfer to other accounts, or move the stolen money through multiple accounts after deposit, and sometimes even transfer it to crypto-asset accounts. • The name of accounts used for these transfers vary, including individual names, corporate names, individual names with trade names, and accounts sold by foreigners when leaving Japan. ＜**Money laundering cases involving online and telephone fraud groups**＞ ○ Transferring swindled money into bank accounts under the names of fictitious or other parties and then withdrawing cash. ○ After transferring the swindled money into bank accounts under the names of fictitious or other parties, the money is either sent to another bank account or a crypto-assets exchange service account controlled by the criminals. ○ Using fraudulently obtained cash cards to operate ATMs, transferring money to bank accounts under the names of fictitious or other parties controlled by the criminals, and then withdrawing cash. ○ Using fraudulently obtained cash cards to operate ATMs, transferring money to crypto-assets exchange service accounts, and depositing it into accounts controlled by the criminals. ○ Selling illegally obtained electronic gift cards (prepaid payment instruments) through websites that mediate the sale of such gift cards and depositing the sales proceeds into an account controlled by the criminals.

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

Offenders	Assessment and Analysis results
Crime Groups of foreigners in Japan	• Criminal proceeds from offences 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 offences, 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 c rime groups existing in their home countries, and these offences tend to be more sophisticated and hidden since the tasks assigned are carried out by different offenders in different countries involved. • Of the cleared money laundering cases in 2022, 108 cases (14.9%) were committed by foreigners in Japan. An examination of cleared cases for money laundering offences over the past three years under the Act on Punishment of Organized Crimes by nationality reveals a significant presence of individuals from China and Vietnam, with China accounting for nearly half of all cases. • Breaking these down by the type of predicate offenses, fraud is the most common, followed by theft and violations of the Immigration Control Act. In terms of offence the type of transaction, domestic exchange transactions are the most common, followed by credit card transactions, cash transactions, and prepaid payment instruments. • With respect to the number of STRs in the last three years, STRs related to Vietnamese and Chinese ranked the highest among other nationalities. Recently, there has been a remarkable increase in reports related to Vietnamese. **[Recent Situation Concerning Crimes Committed by Foreigners in Japan**］ ✓ Situation of Crimes Committed by Vietnamese Nationals in Japan Looking at the cleared money laundering cases involving Vietnamese in Japan by type of predicate offences, fraud is the most common at 26.9%, followed by theft at 20.5%, and Immigration Control Act violations at 19.2%. Additionally, when looking at the types of transactions misused, domestic exchange transactions are the most common at 28.6%. ＜**Common Examples of cleared cases of money laundering offences committed by Vietnamese in Japan**＞ 〇 Operating an underground bank by accepting requests for cross-border remittance through social media and depositing cash into bank accounts under the names of fictitious or other parties opened in Japan. 〇 Depositing sales proceeds from counterfeit residence cards into fictitious bank accounts or those under the names of fictitious or others parties. 〇 Falsifying the product name and sender on the shipping label when sending stolen cosmetics and other items to disposal agents. ✓ Situation of Crimes Committed by Chinese Nationals in Japan Looking at the cleared money laundering cases involving Chinese in Japan by type of predicate offences, theft is the most common at 43.2%, followed by fraud at 36.7%, and computer fraud at 10.8%. When examining the types of misused transactions, credit card misuse is the most common at 25.3%, followed by prepaid payment instruments at 16.0%. ＜**Common Examples of cleared cases of money laundering offences committed by Chinese in Japan**＞ 〇 Created counterfeit cash cards using information obtained through skimming and used them to transfer money to fictitious bank accounts under the names of fictitious or other parties. 〇 An offender received proceeds from credit card payments at an unlicensed adult-entertainment business by making the payments transferred to a bank account under the name of fictitious or other parties. 〇 An offender sold counterfeit goods by using a cash-on-delivery service and made the payments transferred to a bank account under the name of fictitious or other parties to receive criminal proceeds from the sale.

4． Analysis of Money Laundering Cases, etc.（Modus Operandi）1/5

✓ The size of generated criminal proceeds, relevance to money laundering offences, types of misused transactions, danger of fomenting organized crime, impact on sound economic activities, etc., differ depending on the type of predicate offence.

Predicate offences		Assessment and Analysis results
Theft	**Forms of offences/ criminal proceeds**	• There are also cases in which theft is committed continuously and repeatedly by criminal organizations such as Boryokudan and crime groups of foreigners in Japan that result in large amounts of criminal proceeds. • The total financial damages from theft during 2022 was about 58.5 billion yen .
	ML cases	○ Cases where cash obtained through theft is exchanged by an unsuspecting acquaintance and then further disguised as a transfer from the acquaintance to deposit into an account in the name of the perpetrator. ○ Cases that involve purchasing electronic appliances with cash gained from theft and subsequently selling these appliances through a flea market app. ○ Cases where an offender used a flea market app to sell stolen goods in fictious or other party's name and made buyers transfer payments to a bank account under the fictious or other party's name. ○ Cases of buying and keeping stolen cars knowing that they were stolen. ○ 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 offences/ criminal proceeds**	• Frauds, including online and telephone fraud, are repeatedly and continuously committed by domestic and foreign crime groups, generating significant criminal proceeds. • In 2022 , fraud accounted for the highest amount of financial damage, approximately 87.7 billion yen.
	ML cases	○ Cases where housing loan funds are obtained through deception, using forged documents to illegitimately open bank accounts under the name of fictitious or other parties for the deposit of these funds. ○ Cases that involve depositing defrauded money into the perpetrator's account and then using this money to purchase crypto-assets, which are subsequently transferred to a third party's crypto-asset wallet. ○ Cases where an offender opened and misused business accounts under the names of shell companies established for receiving criminal proceeds from fraud targeting public benefits. ○ Cases where an offender opened and misused bank accounts under the name of fictitious or other parties to receive criminal proceeds from fraud.

Predicate offences		Assessment and Analysis results
Computer Fraud	Forms of offences/ criminal proceeds	• 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 fictious or others to accounts managed by the offenders. Some of the cash cards used in computer fraud were illegally obtained through online and telephone fraud. • Losses due to online banking fraud in 2022 were approximately 1.519 billion yen.
	ML cases	○ 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 fictious or other party'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. ○ Cases where, during the application for membership registration in fan clubs online, fraudsters enter stolen credit card information as the payment method for the annual fee, thereby evading payment of the fee.
Violation of the Investment Act/ Money Lending Business Act	Forms of offences/ criminal proceeds	• 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 fictious or other party. • The amount of loss from loan-shark crime committed by offenders who were arrested in 2022 exceeded 5.5 billion yen.
	ML cases	○ Loan sharks required borrowers to send repayments to a post-office box opened under the name of fictious or other party 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 fictious or other party. ○ Loan sharks made a borrower transfer repayments to other borrower's account and made the second borrower send all or part of the repayments to other borrower to lend money to the third borrower.

4. Analysis of Money Laundering Cases, etc.（Modus Operandi） 3/5

Predicate offences		Assessment and Analysis results
Violation of the Immigration Control Act	Forms of offences/ criminal proceeds	• Examples of violations of the Immigration Control Act include 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 (hereinafter referred to as “promotion of illegal employment”). Regarding the promotion of illegal employment, there are cases of trafficking in persons where an offender places foreigners under his/her control by taking away their passports, etc., and forcing them to work. • In cases of forged residence card offences, it has been confirmed that manufacturing bases once located in China have been established within Japan. Under the direction of operatives based in China, various nationalities of residents, including Chinese nationals, were recruited to manufacture forged residence cards within Japan. Since the operatives are located in China, even if manufacturing bases within Japan are exposed and dismantled, they continue to recruit residents, including Chinese nationals, using similar methods and establish new manufacturing bases. Forged residence card offences tend to exhibit a high degree of organization.
	ML cases	• Cases where an offender made purchasers of forged residence cards pay for the cards by transfer to an account under fictious or other party’s name • Cases where an offender received compensation for introducing foreigners remaining in Japan to employers after the expiration of their authorized period of stay as rental income under fictitious residence lease agreements.
Habitual gambling/ Running a gambling venue for profit	Forms of offences/ criminal proceeds	• There are various forms of gambling offences, 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 offences, either directly or indirectly, and gambling is an important source of funds for them. • In 2022, the orders for confiscation were issued against about 3.25 million yen in cash, which was the proceeds from habitual gambling for profit.
	ML cases	• Cases where a gambling offence was committed in an online casino in which money bet by customers had to be paid to an account opened under fictious or other party’s name • Cases where individuals knowingly receive cash under the pretext of leasing gaming machines, knowing that it is part of the proceeds of a criminal act in a gambling establishment.

Predicate offences		Assessment and Analysis results
Violation of the Amusement Business Act/Violation of the Anti-Prostitution Act	Forms of offences/ criminal proceeds	• The reality is that Boryokudanhave been directly or indirectly involved in certain cases. Examples include association with operators of illegal adult-entertainment businesses or sex-related amusement businesses (hereinafter, “adult-entertainment business, etc.”). Criminal proceeds from amusement-related offences 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 of trafficking in persons where offenders forced victims to engage in prostitution by using violence, intimidation, etc. • In 2022, there was a case where bank deposit claims of approximately 59.68 million yen, which were the proceeds made in violation of the Amusement Business Act, became subject to order for confiscation.
	ML cases	• 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 criminal proceeds from prostitution through a bank account under the name of a family member.
Drug-related crimes	Forms of offences/ criminal proceeds	• Evidence gathered in recent years strongly suggests that Boryokudan members 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 orders for confiscation before the institution of prosecution prescribed by the Anti-Drug Special Provisions Law in 2022 was 23. The sum of monetary claims subject to the orders was about 25.36 million yen. Besides monetary claims, properties that became subject to temporary restraining orders for confiscation before the institution of prosecution prescribed by the Anti-Drug Special Provisions Law in the past included vehicles, land, buildings, etc., which indicates that criminal proceeds obtained in cash, etc. are transformed into another type of property.
	ML cases	• Cases where traffickers of stimulants had buyers make payments by transfer to a bank account under the name of fictitious or other parties. • 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, etc.

【Money Laundering etc. related to Ransomware 】

1 About the FATF Report(March 2023)

(1) Current Situation and Characteristics of Ransomware

・Transactions associated with ransomware attacks have rapidly expanded on a global scale in recent years, leading to an increase in money laundering related to ransomware.

・Over half of the victims come from the government sector, public sector, healthcare, industrial products, and services. In recent years, energy, finance, telecommunications, and educational institutions have also become targets.

(2) Characteristics of ML/LF related to Ransomware

・Most ransom payments and subsequent money laundering related to ransomware occur through crypto-assets, with crypto-asset exchanges being commonly used.

・Ransomware attackers leverage the international nature of crypto-assets to conduct large-scale and near-instantaneous cross-border transactions. At times, transactions are carried out without the involvement of financial institutions that implement anti-money laundering/counter-financing of terrorism (AML/CFT) measures.

・Many ransomware networks are connected to countries or regions with a high risk of money laundering, and they deposit or cash out their earnings in such countries or regions.

(3) Measures Required in Each Country

○ Criminalize money laundering related to ransomware.

○ Encourage the private sector, including crypto -assets exchange service providers, to STRs and implement appropriate preventive measures. crypto-assets exchange service providers

○ Strengthen international cooperation. etc.

2. Key Focus Points When Submit STRs

Indicators related to Ransomware Victims' Payments

- Outgoing transfers to cybersecurity consulting companies or incident response companies handling ransomware recovery
- Crypto-asset purchases on behalf of third parties by these companies
- Unusual transfers from insurance companies specializing in ransomware recovery
- Reports from customers regarding ransomware attacks or payments
- Media coverage and reports related to ransomware attacks on customers
- Large transactions from the same bank account to multiple accounts of crypto-assets exchange service providers
- Payment details containing terms like "ransom" or the name of a ransomware group
- Payments to crypto-assets exchange service providers located in high ML/TF (Money Laundering/Terrorist
- Financing) risk countries or regions
- Transactions from customers with no crypto-asset trading history deviating from standard business practices
- Transfers to third parties after customers have raised transfer limits
- Transactions where customers express anxiety or urgency about payment timing
- Purchases of privacy-enhanced crypto-assets
- New customers buy crypto-assets and send account balances to a single address

Indicators related to Ransomware Attackers

- Little or no activity in transactions after the initial large crypto-asset transfer
- Identification of connections to ransomware through blockchain analysis
- Immediate withdrawals after the return of crypto-asset funds
- Sending crypto assets to wallets associated with ransomware
- Utilization of crypto-assets exchange service providers in high ML/TF risk countries or regions
- Sending crypto assets to mixing services
- Use of encrypted networks
- Mention of owning highly private email accounts in customer information
- Inconsistencies in authentication information or requests for account opening with false identity information
- Multiple accounts linked to the same contact with different names
- Transactions related to privacy-enhanced crypto-assets

4． Analysis of Money Laundering Cases, etc.（Misused for ML）

【Major Transactions, etc. Misused for Money Laundering】

Year \ Misused transactions	Domestic exchange transactions	Cash transactions	Deposit transactions	Credit card	Prepaid payment instruments (Note1,2)	Crypto assets	Legal persons	International transaction (such as foreign exchanges)	Funds transfer services	Precious metals and stones	Legal/accounting professionals	Foreign Currency Exchanges	Financial instruments	Total
2020	110	120	96	20	11	32	14	16	1	2	1	1	0	424
2021	208	72	40	40	21	9	16	9	9	2	1	1	2	430
2022	266	105	24	55	39	16	6	7	10	1	1	0	0	530
Total	584	297	160	115	71	57	36	32	20	5	3	2	2	1,384

Note1: Since 2023, the name “electronic money” has been changed to “prepaid payment instruments” in the NRA-FUR.
2: The figures for prepaid payment in 2020 and 2021 include transactions that corresponded to prepaid payment instruments within electronic money.

○ The results of the analysis of the cleared cases of money laundering and STRs

- There were 584 cases of domestic exchange transactions*, followed by 297 cases of cash transactions and 160 cases of deposit transactions, with the majority of transactions misused for money laundering involving products and services offered by deposit-taking financial institutions.
- There are many cases where those who plan to conduct money laundering have victims make payment to bank accounts opened in the name of fictitious or other parties through domestic exchange transactions, which enables prompt and secure fund transfers.
- Ultimately, the criminal proceeds deposited into accounts through domestic exchange transactions or deposit transactions are often cashed out, making subsequent fund tracing extremely challenging.
- With the increase in fraudulent use of credit cards, the number of cases where credit cards were misused for money laundering has also risen.

4． Analysis of Money Laundering Cases, etc.（STR）

✓ Looking at the number of STRs reported in 2022 by business type, the percentage of STRs reported by banks and other deposit-taking institutions was the largest, accounting for 74.7% (435,728) of the total STRs, followed by money-lending companies at 7.8% (45,684) and credit card companies at 7.0% (41,106)

【 Annual Reported Number of STRs by Business Type 】

Category \ Year	2020 Number of reports	2021 Number of reports	2022 Number of reports
Financial institutions, etc.	402,868	495,029	542,003
Deposit-taking institutions	342,226	411,683	435,728
Banks, etc.	319,812	390,381	414,651
Shinkin Banks, Credit Cooperative	19,793	18,461	18,520
Labour Banks	300	318	316
Norinchukin Banks, etc.	2,321	2,523	2,241
Insurance Companies	2,635	3,458	3,939
Financial Instruments Business Operators	17,933	19,718	19,032
Money Lenders	25,255	35,442	45,684
Funds Transfer Service Providers	6,040	10,499	20,271
Crypto-assets Exchange Service Providers	8,023	13,540	16,550
Commodity Derivatives Business Operators	320	388	318
Currency Exchange Operators	252	201	430
Electronic Monetary Claim Recording Institutions	5	7	0
Others	179	93	51
Financial Leasing Operators	123	163	71
Credit Card Operators	29,138	34,904	41,106
Real Estate Brokers	7	4	11
Dealers in Precious Metals and Stones	63	48	124
Postal Receiving Service Providers	2	0	1
Telephone Receiving Service Providers	0	0	0
Telephone Forwarding Service Providers	1	2	1
Total	432,202	530,150	583,317

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

	2020	2021	2022
Number of STRs used for investigation	325,643	353,832	373,849

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
- ✓ Narcotics-related crimes
- ✓ Case of Violation of the Immigration Control Act
- ✓ Case of Violating the Trademark Act
- ✓ Cases of Fraud and Violating the Act on Prevention of Transfer of Criminal Proceeds
- ✓ Case of Violating the Banking Act (Underground Banking)
- ✓ Case of Indecent Electronic Record Transmission and Distribution Incident

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 1/5

✓ 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."

（1） Risk of Transaction Types

Transaction type		Description
Non-face-to-face Transactions	Assessment of Risks	• As non-face-to-face transactions may hinder specified business operators from directly seeing customers and identification documents, the accuracy of customer identification can deteriorate. 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 other person or accounts transferred were misused. Considering this, it is recognized that non-face-to-face transactions present a high risk of being misused for ML/TF.
	Cases	• 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. • A criminal listed illegally duplicated goods on an internet auction site under fictitious names, and received a payment was collected through non-face-to-face transactions using a payment management service on the site.
Cash Transactions	Assessment of Risks	• In general, cash transactions have high liquidity and anonymity. Therefore, cash transactions may hinder the tracing of criminal proceeds. • 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.
	Cases	• Offenders obtained cash by selling or pawning stolen items in the name of a fictitious or another party at secondhand shops, pawnshops, etc. • An offender received criminal proceeds from online and telephone fraud, which were transferred to an account under fictious or other party's name, and withdrew them in cash at an ATM.

（1） Risk of Transaction Types

Transaction type		Description
Cross-border Transactions	Assessment of Risks	• In transactions with foreign countries, it is not easy 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 cross-border transactions. Therefore, it is recognized that cross-border transactions pose a risk of being misused in ML/TF. • It is recognized that the following types of transactions present higher risk: -Transactions related to countries and regions where proper AML/CFT measures are not implemented. - cross-border remittances originated from large amounts of cash.
	Cases	• The modus operandi used in the above cases include “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”, “To use cash couriers”, and “To misuse the transfer of crypto assets”. • 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: ● 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: ● To export goods with export permits obtained by preparing false documents ● 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. In this way, the forms of criminal proceeds change from cash to goods and back to cash again.

（2）Risk of Country/Regions

Assessment of Risks

- The FATF identifies jurisdictions (countries/regions) with strategic AML/CFT deficiencies that have not made sufficient progress in addressing those deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies. It also issues public statements that call on its members to take AML/CFT measures in consideration of risks arising from the deficiencies.
- Those countries/regions identified as High-Risk Jurisdictions subject to a Call for Action have been published as the “blacklist”.

North Korea	Since February 2011 the FATF has continuously called on its members and other jurisdictions to apply countermeasures to protect the international financial system from the ongoing and substantial ML/TF risks emanating from North Korea.
Iran	The FATF requests all member countries, as well as other countries and regions, to completely terminate the temporary suspension of the countermeasures against Iran and apply the countermeasures from February 2020 in light of Iran’s failure to develop internal collateral laws for executing the United Nations Convention against Transnational Organized Crime and international agreements to prevent the provision of funds for terrorism according to the FATF standards.
Myanmar	In its October 2022 statement, the FATF, considering that Myanmar has not made significant progress in addressing serious deficiencies in AML/CFT measures, has called upon all member countries and other jurisdictions to apply enhanced CDD measures commensurate with the risks emanating from Myanmar.

- 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 designated as the Jurisdictions under Increased Monitoring for improving the AML/CFT measures. Transactions conducted with those countries/regions before the deficiencies pointed out by FATF are resolved are recognized to be risky.
- Even if there are no direct transactions with these countries, malicious and shrewd methods may be used to redirect funds through neighboring countries/regions, so thorough measures need to be implemented, including verification at the time of transactions.
- During the FATF plenary meeting in February 2023, it was decided to suspend Russia’s membership in the FATF. This decision was based on the conclusion that Russian Federation’s actions unacceptably run counter to the core principles of the FATF, which aiming to promote security, safety, and the integrity of the global financial system and represented a gross violation of the commitment to international cooperation and mutual respect.

（3）Risk of Customer Attributes 1

Attributes		Assessment of Risks
Boryokudan etc.		• Other than committing various crimes to gain profit, Boryokudan etc. 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 Boryokudan etc. Since Boryokudan etc. engage in money laundering, transactions with Boryokudan etc. are considered to present high risk.
	Anonymous and fluid crime groups	• In recent years, there have also been groups beyond those classified as quasi-Boryokudan that use methods such as recruiting perpetrators through social media, job recruitment websites, etc., to carry out online and telephone fraud, etc. widely, posing a threat to public safety. The police categorize such groups, including quasi-Boryokudan, as “ anonymous and fluid crime groups” and are actively working towards understanding their actual activities. • Anonymous and fluid crime groups are actively engaging in illegal fund-generating activities, such as online and telephone fraud, etc. while coexisting and thriving alongside Boryokudan and others. They use the funds obtained through these activities as capital to expand into various industries, including the adult entertainment industry, the entertainment sector (such as adult videos), and scouting. They also engage in money laundering and serve as a source of talent for online and telephone fraud.
International Terrorists (Such as Islamic Extremists)		• No person of Japanese nationality or residency has been included in the list of persons against whom asset freezing measures are implemented pursuant to the United Nations Security Council resolutions (No. 1267 and succeeding resolutions as well as No. 1373). There have been no terrorist acts carried out in Japan by the terrorists designated by the United Nations Security Council so far. • 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. • It should be recognized as concerns that products and services provided by specified business operators can prevent their monitoring from being misused. 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） Risk of Customer Attributes 2

Attributes	Assessment of Risks
Non-resident Customers	• 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	• 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 (Legal Persons without Transparency of Beneficial Owner, etc.)	• 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 in the form of a legal person, existing stock companies are at 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 a 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 owners present a high risk for ML/TF.

6． Risk of Products and Services 1/8

✓ 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.

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

Assessment of Risks

- Deposit-taking institutions provide various products and services, including accounts, deposit transactions, exchange, safe-deposit, and bills, etc. 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.
- 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.
- Accounts under the fictious or other parties' names are the main criminal infrastructure of ML/TF, among others. Deposit-taking institutions that provide the accounts must take continuous measures to prevent the transfer of accounts and subsequently detect illegal transactions.

Electronic Payment Handling Services, etc.	• Electronic payment handling services, etc., are entities that, on behalf of banks etc., uses electronic data processing systems to reduce the volume of deposit claims equivalent to the transferred funds or to increase the volume of deposit claims equivalent to the funds received through exchange transactions with depositors, etc. who have opened deposit accounts with banks, etc. • The users of electronic payment handling services , etc., are limited to depositors with the respective banks, and various mitigation measures by deposit-taking institutions have also been put in place. As a result, the risk of ML/TF is considered to be reduced to a level comparable to the services provided by deposit-taking institutions.

（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 was 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 misused for ML/TF.

6. Risk of Products and Services 2/8

(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, investments 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 at the 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 had 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.
- In fact, there have been cases where criminal proceeds were transferred overseas through funds transfer services by using third parties who were not involved in predicate offences or by using other 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.
- Considering the increase in both the annual number of remittances and the amount handled in the funds transfer business, the expansion of eligibility for funds transfer service providers to participate in the nationwide bank data communication system (Zengin System), and the deregulation allowing wage payments into the accounts of funds transfer service providers (digital wage payments), the use of funds transfer services as a payment method is expanding. Given this situation, 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.

6. Risk of Products and Services 4/8

（7） Electronic Payment Instruments Dealt with by Electronic Payment Instruments Service Providers

・・・Under the Payment Services Act, electronic payment instruments are defined as currency-denominated assets that can be used for payment to unspecified parties and can be bought and sold with unspecified parties, transferable using electronic data processing systems.

Assessment of Risks
• Electronic payment instruments, similar to Crypto-assets due to their technological similarities, such as the potential use of distributed ledger technology, are recognized to have a high degree of user anonymity and the nature of their transfers being instantaneous and cross-border. • Given that they are more stable in value than Crypto-assets and that considerations for their use in securities settlement are being advanced in Japan, they may be used as a means of remittance and payment in a wide range of fields in the future. Depending on the future circulation in society, including global and technological advancements, the environment surrounding electronic payment instruments could rapidly change, potentially leading to a swift change in their risk level. Considering these factors, the risk of electronic payment instruments being misused for ML/TF is relatively higher compared to other business forms.

（8） Crypto-assets Dealt with by Crypto-assets Exchange 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 under the name of fictious or other party. For this reason, it is considered that crypto-assets are at risk of misuse for ML/TF. • Furthermore, 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 use crypto-asset transactions in addition to products and services handled by deposit-taking institutions. This situation is increasing the degree of risk associated with crypto assets.

（9） 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 ML/TF.
- In fact, 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.

（10） 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. Competent authorities and financial leasing operators are taking, statutory measures as a matter of course, the above-mentioned risk-mitigating measures against these risks.

（11） Credit Cards Dealt with by Credit Card Operators

Assessment of Risks

- Credit cards are recognized as having the risk of misuse for ML/TF because they can transform criminal proceeds obtained in cash into another form of assets by utilizing the credit card and by using fraudulently obtained credit card information to apply for the purchase of goods and then impersonating someone else to receive them, it is possible to disguise the fact of acquiring criminal proceeds.

6. Risk of Products and Services 6/8

(12) 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.
- In fact, there have been some cases where criminal proceeds from prostitution or fraud were used to buy real estate. 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.

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

Assessment of Risks

- Precious metals and stones 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.

(14) 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.
- In fact, there are cases where offenders made contracts 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.

6. Risk of Products and Services 7/8

(15) 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 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.

(16) 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 online and telephone fraud, etc.

(17) 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.
- In fact, there are cases where the services of legal/accounting professionals have been misused to disguise the concealment of criminal proceeds as legitimate transactions. Considering this, it is recognized that when legal/accounting professionals conduct the 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

6. Risk of Products and Services 8/8

【High -Value Electronically Transferable Prepaid Payment Instruments Dealt with by Issuers】

・・・Among prepaid payment instruments for third party business, those capable of electronic value transfer and allowing high-value charges and transfers

Assessment of Risks
• Services allowing charges of tens of millions of yen are also provided by international brand prepaid payment instruments • These international brand prepaid payment instruments, utilizing the payment infrastructure of the brand's credit cards, can be used at affiliated stores of the brand, including online, offering the same service functions as the credit cards, which suggests that they could be considered to have at least the same risk level from an ML/TF perspective. • （Risk Level of Prepaid payment instruments） ✓ With the advancement of cashless payments, the availability of prepaid payment instruments, including online stores, has expanded, and their forms and methods of use are diverse. Furthermore, because identity verification is not required for use, they can be considered to have a high degree of anonymity. ✓ In fact, there have been cases where prepaid payment instruments were misused in the process of money laundering, with an increasing trend in such incidents. ✓ Particularly in cases of online and telephone fraud, criminals deceive victims into giving away their electronic money rights (prepaid payment instruments) and then conceal the criminal proceeds by selling the stolen electronic money rights through websites that mediate the sale and purchase of electronic money.

《Information》 JAFIC website, etc.

○ **JAFIC TOP PAGE**
https://www.npa.go.jp/sosikihanzai/jafic/index.htm

- ◆ **Annual Report and National Risk Assessment Follow-up Report**
  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 (Online and telephone fraud, Organized Crime, Crime Statistics, etc.)**
https://www.npa.go.jp/publications/statistics/index.html

JAFIC
Japan Financial Intelligence Center