November
2025

National Risk Assessment
-Follow-up Report-

[Digest Version]

This document is a digest version of the National Risk Assessment-Follow-up Report (hereinafter referred to as an "NRA-FUR") published in November 2025. It primarily outlines the main revisions, and for more details, refer to the full version of the NRA-FUR.

~Table of Contents~

Section 1. Risk Assessment Method (P.6)

*The page numbers shown in parentheses indicate the corresponding page numbers in the main body of the NRA/FUR (the same applies hereinafter).

*Items (1) to (6) represent the major updates.

Structure of NRA-FUR

Major Updates

(1) Revised the order of descriptions regarding **anonymous and fluid criminal groups**, and the descriptions regarding revenue-generating crimes in light of the current crime environment.

(2) Added a new topic on **online casinos**.

(3) Analyzed **cases of the misuse of corporations and corporate deposit/savings accounts** by criminal groups specializing in ML.

(4) Updated the descriptions regarding **non-face-to-face transactions**, and added a topic on **online banking**.

(5) Updated the descriptions regarding **cross-border transactions**, added new topics on **Trade-based money laundering (TBML)** and threats of fraud based in Southeast Asia.

(6) Established a dedicated chapter on the risk of **terrorist financing**.

[Overview of Assessment*]

Threat		Vulnerability
Offenders		
1. Anonymous and fluid criminal groups 2. Boryokudan (1) 3. Crime groups of foreigners in Japan	Predicate offences (fraud, theft, etc.)	Major transactions misused for money laundering (corporate deposit/savings accounts, domestic exchange transactions, etc.)

○ Risk Assessment (1): High-risk transaction types, countries/regions and customer attributes

Vulnerability: Transaction Types	Countries/Regions	Customer Attributes
1. Non-face-to-face transactions (4) 2. Cash transactions 3. Cross-border transactions (5)	1. Countries/regions where the implementation of countermeasures is requested by the FATF statements Iran, North Korea 2. Countries/regions required to apply enhanced CCD measures commensurate with the risks arising from countries/regions designated by the FATF statement Myanmar	1. Boryokudan 2. Non-resident customers 3. Foreign Politically Exposed Persons (Foreign PEPs) 4. Legal persons (Legal persons without transparency of beneficial owners, etc.) (3)

○ Risk Assessment (2): Products and Services

Products and Services	
Relatively higher risk than other business forms	● Products and services dealt with by deposit-taking institution (excluding those listed below) ● Funds transfer services ● Electronic payment instruments ● Cryptoassets
Transactions considered to be of risk	● Insurance ● Investment ● Trust ● Money lending ● High-value electronically transferable prepaid payment instruments ● Foreign currency exchanges ● Financial leasing ● Credit car ● Real estate ● Precious metals and stones ● Postal receiving services ● Telephone receiving services ● Telephone forwarding services ● Legal/Accounting services

○ Risk concerning terrorist financing

Threat	Vulnerability
Terrorist organizations, including Islamic extremists such as ISIL and AQ, and those involved in terrorist financing	Legal and illegal sources and means of terrorist financing

*Money laundering and terrorist financing differ in the following respects, among others: (i) terrorist financing does not always involve funds obtained by illegal means; (ii) transactions related to terrorist financing could be smaller in amount than those related to money laundering; and (iii) the countries/regions that require attention as remittance destinations may be different between money laundering and terrorist financing. The NRA-FUR describes risks based on these differences. In addition, because terrorist financing itself is a crime and terrorist funds themselves can be criminal proceeds subject to money laundering, it is considered that those who try to finance terrorists attempt to conceal the transfer of funds, like other criminal proceeds, by misusing various transactions and products/services. Thus, the risks in transactions and products/services described in the NRA-FUR include terrorist financing risks.

Section 1. Risk Assessment Method (P.6)

1. History **2. Purpose** 3. Assessment Method 4. Updates to the NRA-FUR

○ History (P.6)

Event	Details
(1) February 2012 FATF New Recommendations	In Recommendation 1, FATF requests countries to "identify and assess money laundering and terrorist financing risks for the country"
(2) June 2013 G8 Action Plan Principles	In the G8 Lough Erne Summit, G8 Action Plan Principles were agreed on which stipulated that each country should "understand the risks to which their anti-money laundering and countering the financing of terrorism regime is exposed, and implement effective and proportionate measures to target those risks"
(3) June 2013 Japan's Action Plan	In accord with the FATF Recommendations and the G8 Action Plan Principles, Japan set up a working group, which consisted of the National Police Agency and other relevant ministries and agencies, including the Financial Services Agency, and formulated the action plan that includes conducting a national risk assessment on AML/CFT by the end of 2014

National Risk Assessment-Baseline Analysis (NRA: National Risk Assessment)
(Published in December 2014)

(4) November 2014 Amendment to the Act on Prevention of Transfer of Criminal Proceeds	Under the provisions of Article 3, paragraph (3) of the Act on Prevention of Transfer of Criminal Proceeds, newly established by the amendment to the Act, the National Public Safety Commission is required to prepare and publish NRA-FUR describing risks, etc. in each category of the transactions carried out by specified business operators, on an annual basis

National Risk Assessment-Follow-up Report (NRA-Follow Up Report)
(Prepared and published annually from 2015 onward)

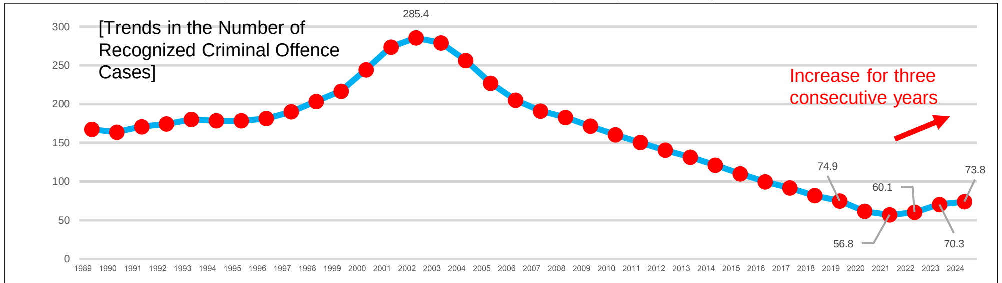
○ Purpose (P.7)

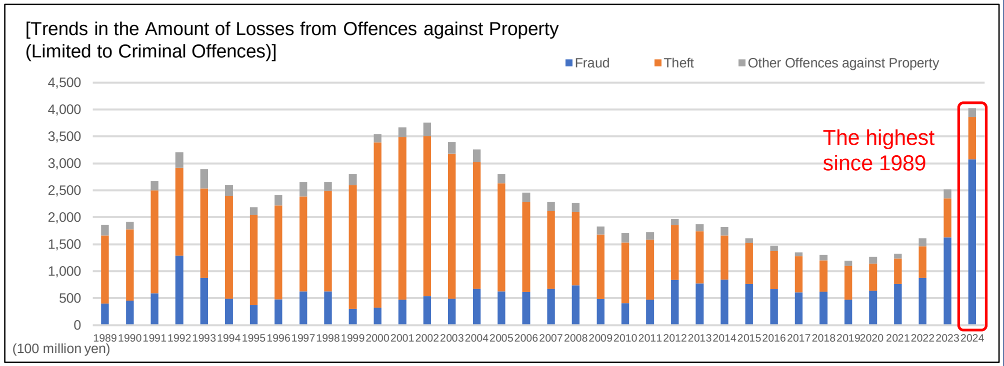
- The purpose of the NRA-FUR is to identify and assess the risks of specific types of transactions conducted by specified business operators being misused for ML/TF
- Specified business operators are required to take into consideration the contents of the NRA-FUR, determine whether there is any suspicion of ML/TF, and submit suspicious transaction report (STR), as well as take measures to properly conduct verification at the time of transaction, etc. in order to **effectively prevent the products and services they handle from being misused for the transfer of criminal proceeds**
- The NRA-FUR serves as the premise for effective and efficient AML/CFT measures based on a **risk-based approach** taken by specified business operators.

1. Geographic Environment 2. Social Environment 3. Economic Environment **4. Criminal Environment**

Number of Recognized Criminal Offence Cases (P.13)

- Total number of recognized criminal offence cases has increased for three consecutive years since 2021
- The amount of losses from offences against property is the highest since 1989
- Among offences against property, the amount of losses from fraud has increased sharply compared to the previous year (+89.1%)



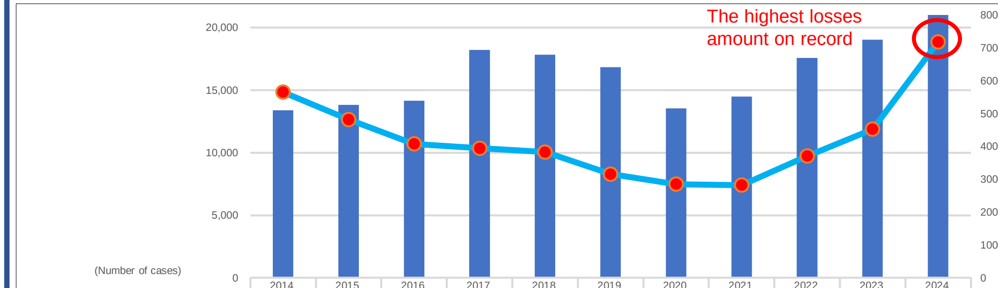


Amount of losses (100 million yen)	2019	2020	2021	2022	2023	2024
Fraud	469.5	640.1	763.0	876.8	1,625.8	+89.1% 3,074.7
Theft	633.2	501.6	474.0	585.3	725.8	789.3
Other Offences against Property	90.6	125.3	89.5	145.8	167.4	156.6
Total	1,193.3	1,267.0	1,326.5	1,607.8	2,519.1	4,020.7

The highest since 1989

Fraud (Online and telephone fraud and investment/romance fraud via social media) (P.15)

- Online and telephone fraud: Both the number of recognized cases and the amount of losses have increased, with the amount of losses reaching a record high
- In “It’s me” fraud, losses from fake police fraud are particularly prominent



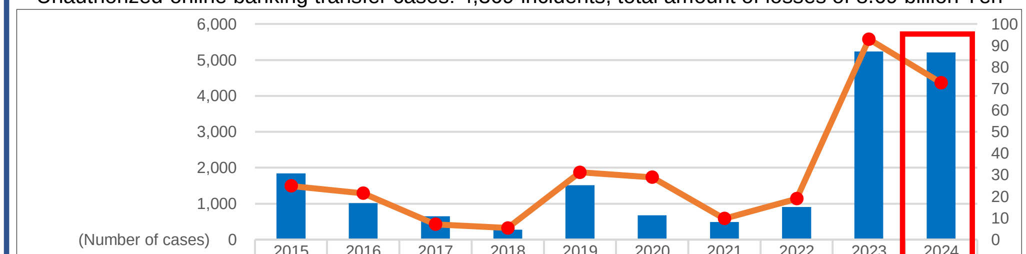
	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Number of recognized case	13,392	13,824	14,154	18,212	17,844	16,851	13,550	14,498	17,570	19,038	21,043
Amount of losses	565.5	482.0	407.7	394.7	382.9	315.8	285.2	282.0	370.8	452.6	718.8

- Investment/romance fraud via social media: Both the number of recognized cases and the amount of losses have increased sharply

Offence	2023		2024	
	Number of recognized case	Amount of losses (100 million yen)	Number of recognized case	Amount of losses (100 million yen)
Investment fraud via social media	2,271	277.9	6,413	871.1
Romance fraud via social media	1,575	177.3	3,824	400.9
Total	3,846	455.2	10,237	1271.9

Cyber Crimes (P.18)

- Unauthorized online banking transfer cases: 4,369 incidents, total amount of losses of 8.69 billion Yen



	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Amount of losses	30.7	16.9	10.8	4.6	25.2	11.3	8.2	15.2	87.3	86.9
Number of incident	1,495	1,291	425	322	1,872	1,734	584	1,136	5,578	4,369

Section 2. Environment Surrounding Japan (P.12)

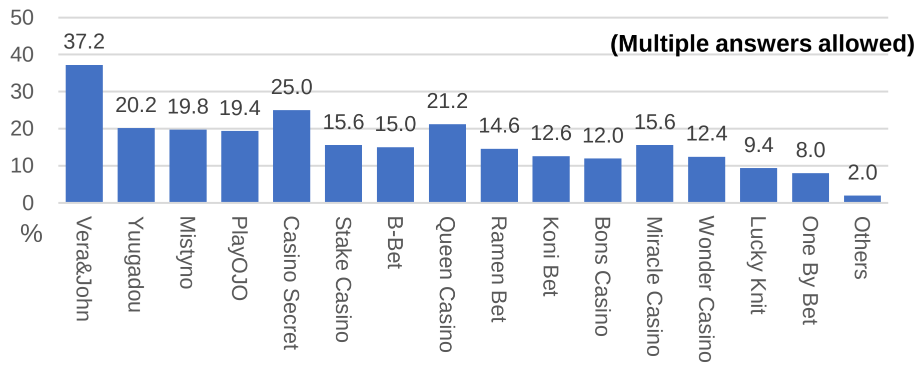
- There are cases where online casinos are being used domestically, and ML is being carried out using the online casino system

***Accessing online casinos from within Japan to engage in gambling constitutes a crime**

The National Police Agency has commissioned a private contractor to ascertain the actual usage of online casinos and gather information on the sites, and published, the "Outsourced Research Report on Research Study to Understand the Actual State of Online Casinos" in March 2025

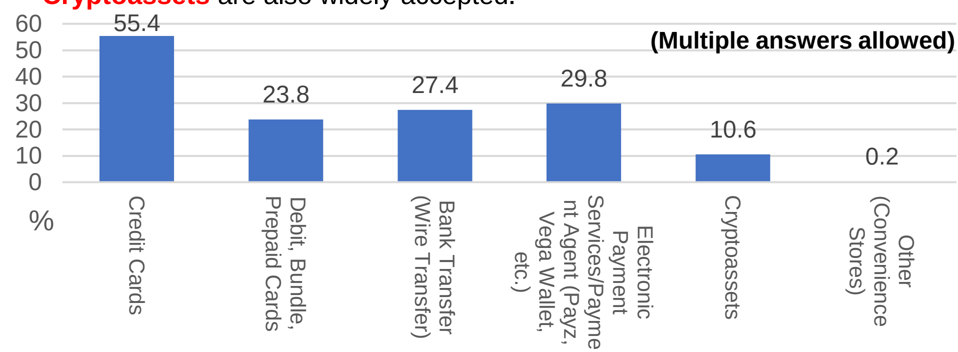
Online Casino Sites Confirmed to Be Used from within Japan

- The online casino sites surveyed are operated under licenses obtained abroad
- Licenses from Curacao account for the majority of the 40 sites surveyed



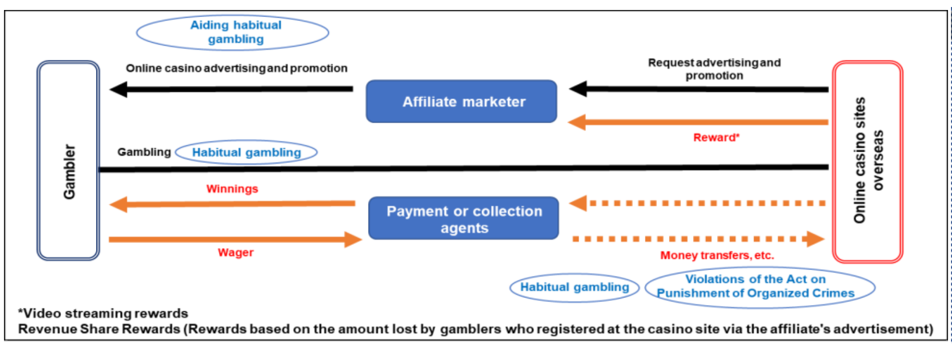
Deposit Methods for Online Casinos

- Various options exist for depositing funds, including credit cards and electronic payment services, with the characteristics that deposits are reflected immediately. **Cryptoassets** are also widely accepted.



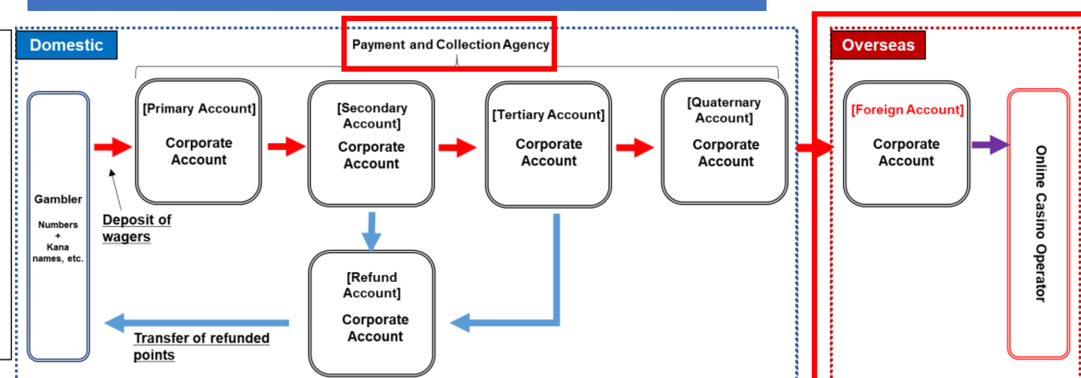
The following revenue structures and flows of funds are observed for online casinos.

Examples of Revenue Structures Related to Online Casinos



- Funds flow to online casino site operators through accounts held by entities **referring to themselves as payment or collection agents**(*).
  *There have been cases where such entities were arrested for habitual gambling or violations of the Act on Punishment of Organized Crimes and Control of Proceeds of Crime

Illustration of Flow of Funds Related to Online Casinos



- There are some cases where, funds pass through multiple corporate accounts held by entities referring themselves as payment or collection agents, and are ultimately transferred to accounts located overseas.

Section 3. Analysis of Money Laundering Cases (P.30)

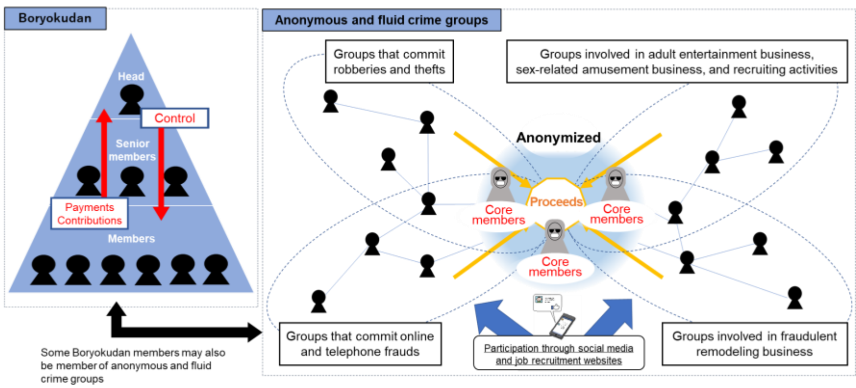
1. Offenders 2. Predicate Offences 3. Major Transactions Misused for Money Laundering 4. Suspicious Transaction Report (STR)

(1) Anonymous and fluid criminal groups (P.31) (2) Boryokudan (3) Crime Groups of Foreigners in Japan

➢ In light of the current crime environment and its impact on sound economic activities, the order of descriptions regarding offenders were revised and **"anonymous and fluid criminal groups"** were placed at the beginning. The descriptions regarding revenue-generating crimes have also been updated

Characteristics

- Anonymity of core members and fluidity of crime actors
- Diverse revenue-generating activities and the return of criminal proceeds
- While there are some relationships between Boryokudan and Anonymous and fluid criminal groups, it appears that there are also individuals who act as hubs between the two



Revenue-generating Crimes

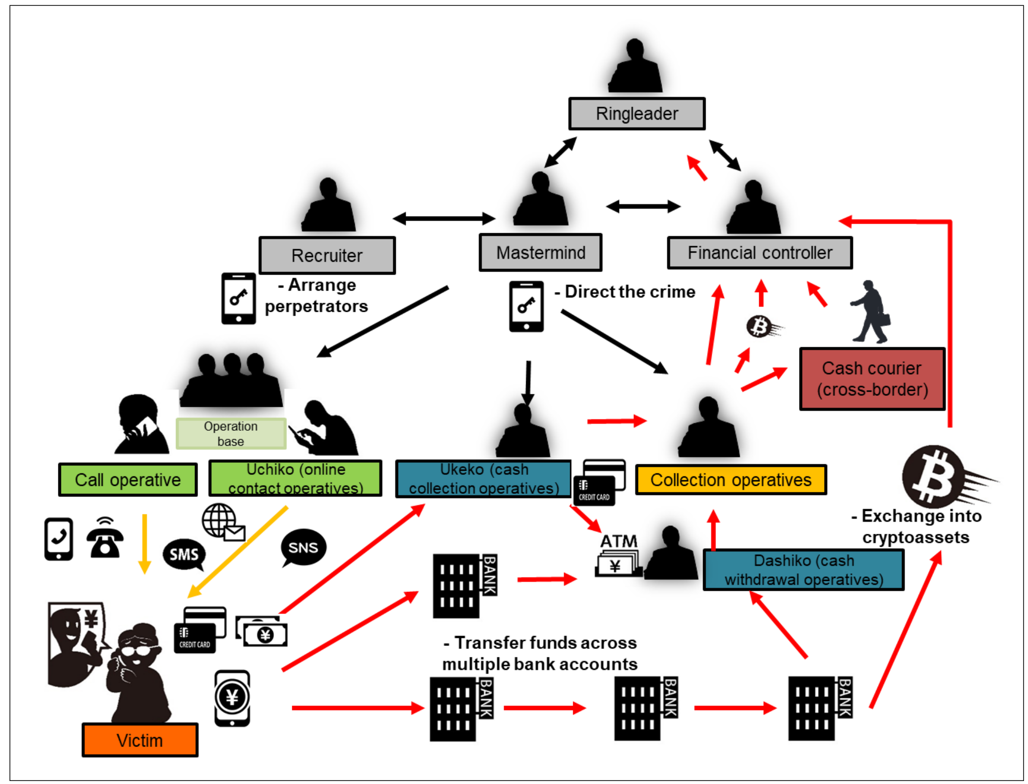
Anonymous and fluid criminal groups are involved in wide range of cases and are **engaged in a variety of revenue-generation**

- Organized robbery
- Online and telephone fraud
- Investment/romance fraud via social media
- Organized theft and trafficking of stolen goods
- Malicious host club offences and amusement-related offences
- Gambling offences conducted online
- Online banking fraud cases
- Specified commercial transactions by malicious remodeling businesses, etc.

Modus Operandi of ML cases

When anonymous and fluid criminal groups launder criminal proceeds obtained through online and telephone fraud, the flow of funds can be illustrated as shown in the table below.

- The funds ultimately reach core members such as ringleaders
- In some cases, **core members are located at bases overseas**
- There are also cases where criminal proceeds are transferred abroad through means such as foreign remittances, cryptoassets, or cash couriers



Section 3. Analysis of Money Laundering Cases (P.30)

1. Offenders **2. Predicate Offences** **3. Major Transactions Misused for Money Laundering** 4. Suspicious Transaction Report (STR)

The Number of Cleared ML Cases (P.30)

	2022	2023	2024
Violations of the Act on Punishment of Organized Crimes	709	888	1,262
Violations of the Anti-Drug Special Provisions Act	17	21	21
Total	726	909	1,283

Measures to combat crimes facilitating the misuse of deposit/savings accounts (P.58)

In ML cases, **fictitious or third-party accounts** serve as a primary criminal infrastructure. The police are actively cracking down on crimes that promote the misuse of corporate deposit/savings accounts

[Number of Cleared Cases of the Violation of the Act on Prevention of Transfer of Criminal Proceeds]

Category		2022	2023	2024
Transfer of passbooks and other deposit instruments	(cases)	2,951	3,230	4,321
Transfer of passbooks and other deposit instruments (business)	(cases)	18	43	29
Solicitation or inducement for the transfer of passbooks and other deposit instruments	(cases)	10	12	12
Transfer of foreign exchange transaction cards and similar instruments	(cases)	41	50	60
Provision of information for cryptoasset exchanges	(cases)	46	89	90
Other	(cases)	0	0	1
Total	(cases)	3,066	3,424	4,513

- Among the nationality of suspects, Japan accounts for the highest number, followed by Vietnam and China.
- There are cases where accounts fraudulently transferred by foreign residents returning to their home countries were misused.
- In addition to transferring accounts, another scheme involves providing others with account information and then transferring funds deposited into one's account to designated separate account.
- It can be inferred that **the number of transferred accounts far exceeds the number of cleared cases**

The Police request account freezes from financial institutions managing the accounts whenever losses from online and telephone fraud or similar crimes is recognized. There have been cases in which, with respect to such frozen accounts, applications for attachment of claims were filed with the court based on false payment demands or notarized deeds, and funds were withdrawn through compulsory execution.
The corporate representatives who submitted the applications for attachment of claims have been prosecuted for fraud and for making false statements in, and using, notarized deeds.

Numbers of Cleared ML Cases Categorized by Predicate Offence (P.45)

- Fraud and computer fraud together account for approximately 50% of the total.
- As the incidence of online and telephone fraud has increased, the number of ML cases with these offences as predicate offences has also risen.

*For notes in the table, please refer to the main text

Year \ Predicate Offences	Fraud	Theft	Computer fraud	Drug-related offences (Note 1)	Violation of the Investment Act/Money Lending Business Act (Note 2)	Habitual gambling/ running a gambling venue for profit	Violation of the Trademark Act (Note 3)	Violation of the Amusement Business Act	Document forgery offences (Note 4)	Extortion	Violation of the Immigration Control and Refugee Recognition Act	Violation of the Anti-Prostitution Act (Note 5)	Embezzlement	Violation of the Financial Instruments and Exchange Act	Other	Total
2022 (cases)	254	257	105	21	13	11	10	4	12	8	7	4	6	1	40	753
2023 (cases)	334	319	160	22	16	17	9	9	9	5	6	5	6	6	32	955
2024 (cases)	462	386	288	24	24	16	13	14	3	9	7	11	8	4	46	1,315
Total (cases)	1,050	962	553	67	53	44	32	27	24	22	20	20	20	11	118	3,023

Major Transactions Misused for Money Laundering (P.56)

- Products and services dealt with by deposit-taking institutions (domestic exchange transactions and deposit transactions) account for approximately 60% of the total.
- In cases involving the misuse of cash transactions, the majority involve converting criminal proceeds, such as stolen goods, into cash by selling them to buyers.
- Most cases of the misuse of credit cards involve the fraudulent use.

*For notes in the table, please refer to the main text

Year \ Misused transactions	Domestic exchange transactions	Cash transactions (Sale of stolen goods, etc.) (Note 1)	Credit cards	Prepaid payment instruments (Note 2)	Deposit transactions	Cryptoassets	Legal Persons	Funds transfer services	Cross-border Transactions (such as foreign exchanges)	Financial instruments	Precious metals and stones	Electronic payment instruments (Note 3)	Real estate	Money lending	Foreign currency exchange	Legal/accounting professionals	Bills and checks	Postal receiving services	Total
2022 (cases)	266	80	55	39	24	16	6	10	7	0	1	-	0	0	0	1	0	0	505
2023 (cases)	311	89	51	40	36	29	15	21	11	3	3	-	4	2	2	0	1	1	619
2024 (cases)	551	101	73	36	29	43	35	10	5	4	2	6	1	2	1	1	0	0	900
Total (cases)	1,128	270	179	115	89	88	56	41	23	7	6	6	5	4	3	2	1	1	2,024

Section 3. Analysis of Money Laundering Cases (P.60)

1. Offenders 2. Predicate Offences 3. Major Transactions Misused for Money Laundering **4. Suspicious Transaction Report (STR)**

- Against the backdrop of heightened awareness of AML/CFT and the advancement of monitoring systems among specified business operators, the number of **STRs has been on an upward trend**.
- With respect to specified business operators in the non-financial sector, such as real estate agents, dealers in precious metals and stones, and postal receiving service providers, the number of STRs has increased; however, their overall share of the total remains low.
- STRs that specifically describe the grounds for suspicion and are accompanied by supporting materials such as transaction statements are useful for analysis and investigation and are considered to be high-quality reports.

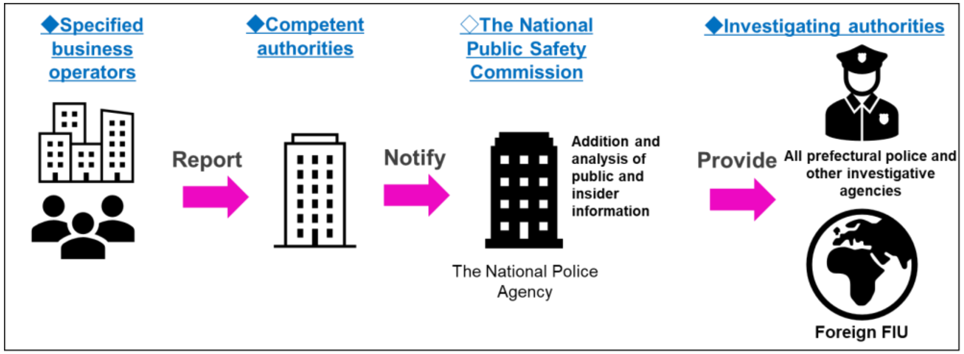
Annual Reported Number of STRs by Business Type (P.61)

*For notes in the table, please refer to the main text

Category \ Year	2022	2023	2024		
	Number of reports	Number of reports	Number of reports	Share of the total (%)	Year-on-Year (%)
Financial institutions	542,003	661,838	791,440	93.13	+19.6
Deposit-taking institutions	435,728	522,649	611,069	71.90	+16.9
Banks (Note 1)	414,651	498,155	580,382	68.29	+16.5
Shinkin banks, credit cooperative	18,520	21,636	24,925	2.93	+15.2
Labour banks	316	397	1,370	0.16	+245.1
Norinchukin banks, etc.(Note 2)	2,241	2,461	4,392	0.52	+78.5
Insurance companies	3,939	4,575	5,428	0.64	+18.6
Financial instruments business operators	19,032	20,550	23,804	2.80	+15.8
Money lenders	45,684	63,954	88,282	10.39	+38.0
Funds transfer service providers	20,271	29,232	39,122	4.60	+33.8
Cryptoassets exchange service providers	16,550	19,344	22,667	2.67	+17.2
Commodity derivatives business operators	318	846	428	0.05	-49.4
Currency exchange operators	430	655	617	0.07	-5.8
Electronic monetary claim recording institutions	0	14	3	0.00	-78.6
Other (Note 3)	51	19	20	0.00	+5.3
Financial leasing operators	71	214	141	0.02	-34.1
Credit card operators	41,106	45,674	57,978	6.82	+26.9
Real estate brokers	11	18	25	0.00	+38.9
Dealers in precious metals and stones	124	138	223	0.03	+61.6
Postal receiving service providers	1	30	35	0.00	+16.7
Telephone receiving service providers	0	0	0	-	-
Telephone forwarding service providers	1	17	5	0.00	-70.6
Other (Note 4)	-	-	14	0.00	-
Total	583,317	707,929	849,861	100.00	+20.0

Flow of Information on Suspicious Transactions (P.62)

- The National Public Safety Commission and National Police Agency collect, organize and analyze the STRs and **provide the prefectural police and other investigative organizations** with those that are considered to be useful for investigating ML offences or their predicate offences
- Information on suspicious transactions is widely utilized in investigations and related activities



Number of Reports Provided to Investigating Authorities and Oher Authorities (P.62)

	2022	2023	2024
Number of information provide related to STRs (cases)	581,252	685,330	815,318
Number of analytical results provided (cases)	15,990	21,730	26,871

Number of Information on Suspicious Transactions Utilized in Investigations and Other Activities (P.62)

	2022	2023	2024
Number of Information on Suspicious Transactions Utilized in Investigations and Other Activities (cases)	373,849	496,093	629,135

Section 3. Analysis of Money Laundering Cases (P.60)

- **Information on suspicious transactions is effectively utilized in investigations of ML offences**
  Examples of cleared cases detected through STRs by the prefectural police (17 cases) and examples of cases in which other investigating authorities utilized STRs (5 cases) are described.

Examples of Cleared Cases Detected through STRs by the Prefectural Police (P.63)

Case Name	Fraud cases
Business type of the reporter	Deposit-taking institution, Cryptoassets exchange service providers
Reported account	Accounts in the name of Japanese and accounts in the names of their relatives
Reason for Report	**<Deposit-taking institution>** - A large number of deposits from multiple corporate entities and individuals were suddenly made into an account that had been inactive for a certain period - Multiple deposits, including from legal persons, were received, followed by transfers to numerous accounts via online banking or cash withdrawals from ATMs - Login information in a foreign language, different from usual, was detected in the bank's app, suggesting suspicious activity possibly to verify the functionality of an account intended for transfer **<Cryptoassets exchange service providers>** - A report was received from another financial institution indicating that the account in question is being used for fraudulent transactions
Investigation results	It was confirmed that the account holder opened the account for the purpose of allowing third parties to use it and had transferred multiple accounts to such third parties for consideration, and the account holder was subsequently arrested

Case Name	Gambling offences (online casino)
Business type of the reporter	Deposit-taking institution, Cryptoassets exchange service providers
Reported account	Account in the name of Japanese
Reason for Report	**<Deposit-taking institution>** - Determined to be an online casino user based on the IP address and the counterparty's account - Usage of the bank app was observed from the same IP address as another account with a different account holder and address, raising suspicion of third-party use of the account **<Cryptoassets exchange service providers>** - Within a short period, there were frequent receipts of cryptoassets and cash deposits. The cryptoassets were traded, followed by cash withdrawals to the registered account and transfers of cryptoassets to external addresses under the same owner. A portion of the received cryptoassets was transferred to external addresses without being traded even once, indicating unusual activity
Investigation results	It was confirmed that the account holder had engaged in gambling through an online casino, and the individual was subsequently arrested

Section 4. Risk of Transaction Types, Countries/Regions, and Customer Attributes (P.71)

1. Transaction Types (1) Non-Face-to-face (2) Cash Transactions (3) Cross-border Transactions

Non-Face-to-Face Transaction (P.71)

[Inherent Risks of Being Misused for ML/TF]

- **Online non-face-to-face transactions have been increasing rapidly**
- Difficult to verify the individual's identity through appearance, behavior, or other in-person cues
- Accuracy of verification at the time of the transaction tends to be decreased
- In a non-face-to-face environment, even if corporate deposit/saving accounts or other accounts are transferred or lent to third parties and transactions are conducted by persons other than the contractual holder, specified business operators cannot easily identify such situations

[Measures Taken by Business Operators]

➢ Conducting **ongoing monitoring** after the completion of verification at the time of transaction, **taking into account the possibility for unauthorized transactions by third parties**

(Specific measures)

- Verification of the consistency of login IP addresses, access locations, browser language settings, and device information
- Confirmation of customers' registered information such as phone numbers and email addresses
- Conduct of 24/7 transaction monitoring
- Detection of changes to registered contact information or transfer limits
- Monitoring of transactions with attention to signs such as unusual login frequency or unnatural fund movements

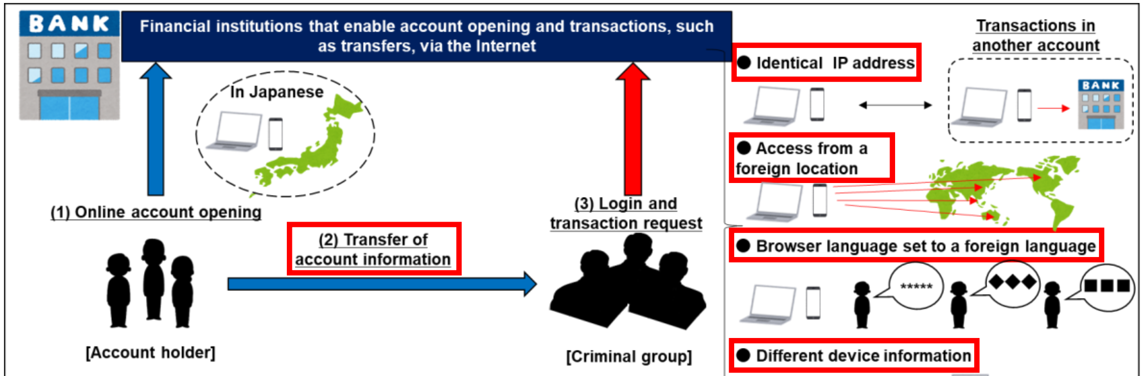
[Statutory Measures]

➢ Among methods of non-face-to-face verification of identification matters, **abolished the method carrying a high risk of impersonation through forgery or alteration of identification documents**

→ Partial amendment to the Ordinance of the Act on the Prevention of Transfer of Criminal Proceeds: Promulgated in June 2025 and scheduled to come into force in April 2027

➢ Even in face-to-face, there are cases where forged or altered identification documents are misused

→ Revisions to the relevant provisions of the Ordinance of the Act on the Prevention of Transfer of Criminal Proceeds are being considered to, **in principle**, require that face-to-face verification of identification matters involve **not only the presentation of identification documents with a photograph and an IC chip but also the reading of IC chip information**



(Examples of Detecting Suspected Unauthorized Transactions by Third Parties in Non-Face-to-Face Transactions)

[Topic] Fraudulent Transfers, Online and Telephone Fraud, Investment/Romance Fraud via Social Media Misusing Online Banking (P.76)

●Special fraud

→ Survey on **transfer-type** cases in 2024 involving **losses of 5 million yen or more** (1,673 recognized cases, with total amount of losses of 30.77 billion yen)

- Percentage of use of online banking: **approximately 60%** of the number of recognized cases and **approximately 70%** of the total amount of losses
  Both the number of recognized cases and the amount of losses involving the use of online banking are on an upward trend
- Approximately 70% involved accounts for which victims had set up online banking functions prior to becoming a victim
- There were confirmed cases where victims, under the suspect's instructions, opened online banking accounts or additionally enabled online banking functions, as well as cases where suspects opened such accounts in the victims' names

●Investment/romance fraud via social media

→ Survey on **transfer-type** cases in 2024 involving losses of 5 million yen or more (8,349 recognized cases, with total amount of losses of 107.43 billion yen)

- Percentage of use of online banking: **approximately 60%** of the number of recognized cases and **about 70%** of the total amount of losses

Online banking transaction limits can be changed without face-to-face manner
Transfers over consecutive days have contributed to higher amounts of losses
[Measures to Mitigate Risks by Specified Business Operators]

- **Appropriately setting initial transaction limits**
- **Providing confirmation and warnings to users when applying for online banking or when raising limits**

Section 4. Risk of Transaction Types, Countries/Regions, and Customer Attributes (P.71)

1. Transaction Types (1) Non-Face-to-face (2) Cash Transactions **(3) Cross-border Transactions**

Cross-Border Transaction (P.83)

[Inherent Risks of Being Misused for ML/TF]

- Cross-border transactions have the nature that making it more difficult to track the transfer of funds compared to domestic transactions
- Advances in IT technology have diversified payment methods and ways to transfer funds abroad
- In addition to cross-border exchange transactions conducted through banks, instant foreign remittance using funds transfer service providers or cryptoassets are now being utilized

[Modus Operandi of ML]

(1) Misuse financial institutions in Japan and abroad (e.g., cross-border remittances) while **disguising the purpose of the sending or receiving funds**

(2) **Disguising ML as legitimate trading** (e.g., export or import of goods)

(3) Provision of domestic and cross-border remittance and payment services without actually moving funds **(so-called "underground banking")**

(4) Use **cash couriers** (cash transportation)

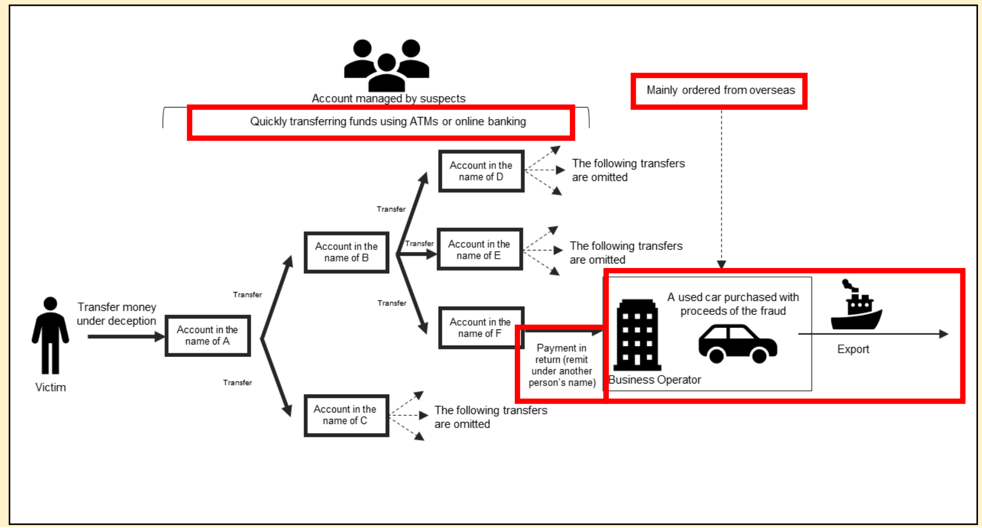
(5) Misuse of transfer of **cryptoassets**

[Topic] Analysis of Trade-Based Money Laundering (TBML) (P.92)

➢ **Cases where the funds obtained from online and telephone fraud are routed through multiple bank accounts controlled by the suspects before being deposited as payment for used cars into the accounts of business operators engaged in the sale and export of used cars**

<Characteristics>

- Large amounts of funds are transferred to used car dealers within a short period of time after passing through multiple bank accounts.
- In one case, approximately 30 minutes elapsed between the victim's losses from online and telephone fraud and the deposit into the used car dealer's account
- Bank accounts in the names of foreigner are primarily used, with a relatively high proportion involving Vietnamese nationals in particular. There have also been cases where bank accounts belonging to individuals who had already returned to their home countries were used.
- When funds are deposited into the used car dealer's account, it is often observed that the account name is altered to another foreign name or to a string of numbers.



[Topic] Threats of International Fraud and ML Based in Southeast Asia (P.93)

➢ Introducing the report published by UNODC in April 2025.
The report revealed that **scam centers based in Southeast Asia** function as major money laundering hubs, handling an estimated US$40 billion, under structures combining human trafficking, forced labor, cryptoassets, underground banking, and related mechanisms

- As the online criminal industry in Southeast Asia continues to expand, dedicated business parks serving as operational bases have been developed
- A characteristic is its mobility. Due to external factors such as law enforcement pressure and conflict, operations and workers relocate within countries or across borders

The report includes locations of **scam centers** identified or reported in the **Mekong region**

3. Customer Attributes (1) Boryokudan (2) Non-resident Customers (3) Foreign Politically Exposed Persons **(4) Legal Persons (P.106)**
[Topic] Analysis of Criminal Groups Engaged in ML Using Corporations (P.113)

- In cases of ML involving the misuse of corporations, the following examples have been identified:
  - **A shell company is established** to open a corporate account and conduct rapid inflows and outflows of funds.
  - **Dormant companies or corporate bank accounts are purchased** and used.
  - Mixing criminal proceeds with **revenues of legitimately operating corporations**
  - Providing fund transfer services through **payment and collection agencies**
  - The funds circulated have included criminal proceeds related to online and telephone fraud, investment/romance fraud via social media, and online casino activities
- Establishment of a corporation and account management handled by someone other than the actual operators, and unclear corporate activities or fund flows, can constitute risk factors.

[Topic] Analysis of Criminal Groups Engaged in ML Using Corporations (P.113)

In recent years, it has become evident that **there are criminal groups that handle the ML of proceeds from crimes** committed by other groups, such as online and telephone fraud. It analyzes the characteristics of the corporations, accounts, and transactions used by these criminal groups.

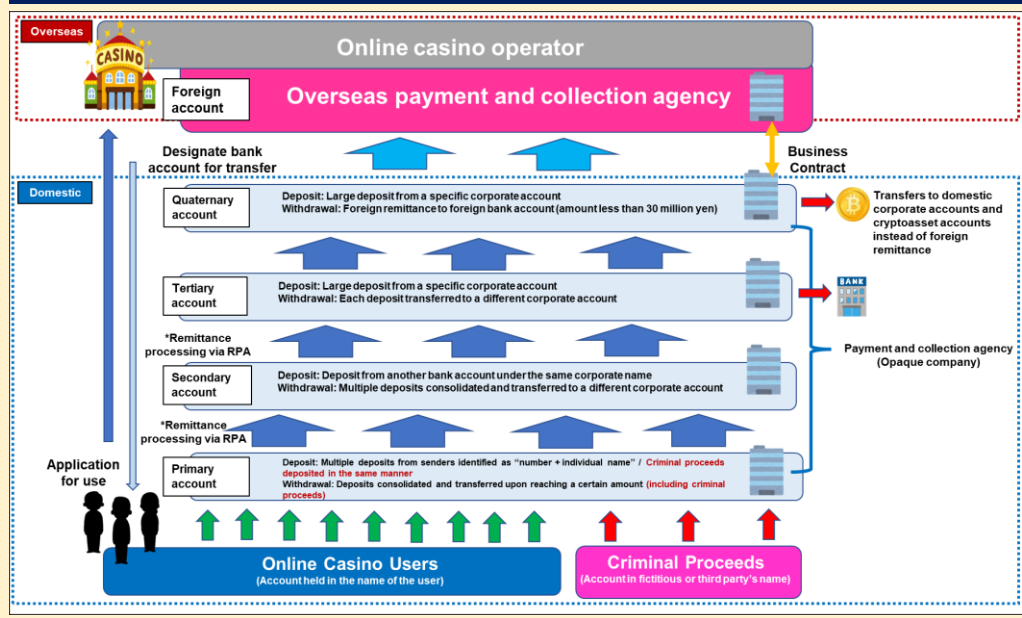
Analysis Results Concerning Accounts

- A single corporation opens accounts at multiple banks (with the involvement of an instructor)

Analysis Results Concerning Remittance Transactions

- Funds deposited into an initial account (primary account) were quickly transferred to another account (secondary account), then routed through multiple intermediary accounts (tertiary accounts), and ultimately transferred to an account used for foreign remittances (quaternary account).
- Some transactions involved transfers to financial institution accounts of cryptoassets exchange service providers or cash withdrawals via ATMs.
- In some cases, RPA is used to automate the transfer process.
- Repeated foreign remittances of less than 30 million yen.

Illustration of ML Using Corporate Account (Utilizing the Mechanism of Online Casinos)



Section 5. Risk of Products and Services (P.118)

Risk of Products and Services Dealt with by Specified Business Operators

Risk	Products and Services
Transactions of relatively higher risk than other business forms	Products/services provided by deposit-taking institutions (excluding those listed in the table below), funds transfer services, electronic payment instruments, and cryptoassets
Transactions considered to be of risk	Insurance, investment, trust, money lending, high-value electronically transferable prepaid payment instruments, foreign currency exchanges, financial leasing, credit cards, real estate, precious metals and stones, postal receiving services, telephone receiving services, telephone forwarding services, and legal/accounting services

Structure of Chapter 5

* This digest version explains the structure and its contents. For details of each product and service, please refer to the main text.

(i) Factors that Increase Risks

(A) Inherent Risks of Being Misused for ML/TF

→ Overview, scale, characteristics, and vulnerabilities of each product and service

b Typologies

→ Introduction of cases misused for ML

(ii) Trends of STRs

→ The number of reports submitted over the past three years and reasons for submitting reports that recorded the highest number of reports (guideline numbers and names in the “Guidance for Submitting STRs”)

(iii) Measures to Mitigate Risks

(A) Statutory Measures

→ Regulatory requirements stipulated under the Act on Prevention of Transfer of Criminal Proceeds and other relevant industry laws

(B) Measures by competent authorities

→ Guidelines established and examples of specific initiatives taken by the competent authorities

(C) Measures by industry associations and business operators

→ Specific initiatives taken by the industry associations and business operators

(iv) Items That the Competent Authorities Have Identified and That Business Operators Should Be Aware Of

→ Matters that business operators are required to take into consideration by the competent authorities

(v) Assessment of Risks

→ Results of the risk assessment and transactions at a higher risk

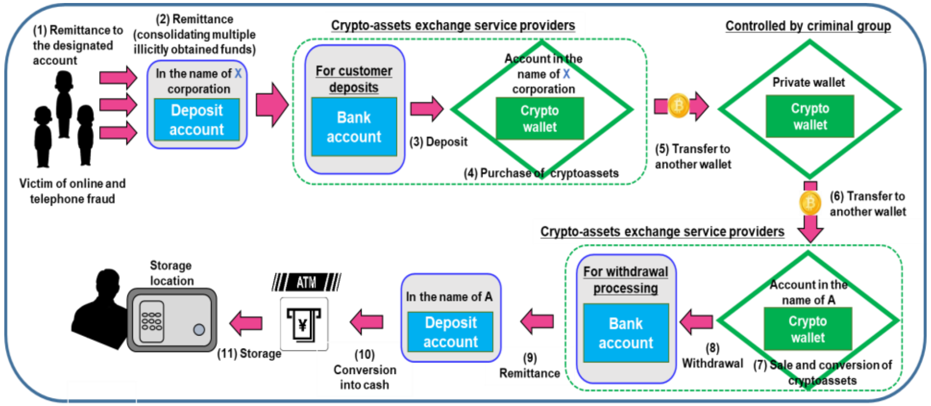
Section 5. Risk of Products and Services (P.118)

(i) Factors that Increase Risks (A) Inherent Risks (B) Typologies

➢ Common examples of misusing each product and service for ML are described
The following are excerpts of the main illustrative tables included in the report

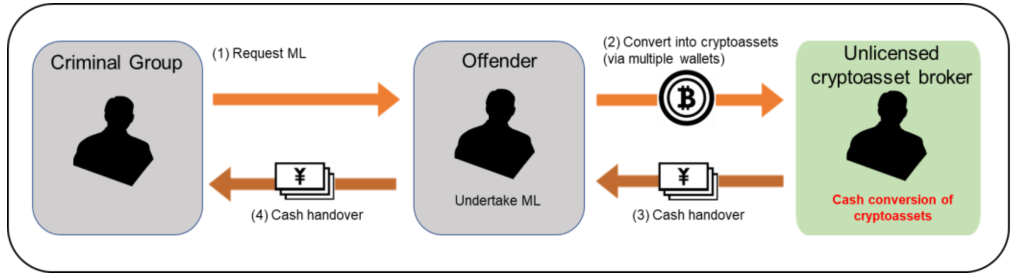
(9) Cryptoassets Dealt with by Cryptoassets Exchange Service Providers (P.166)

[Flow of Money Laundering Involving Abuse of Cryptoassets]



→ A case in which funds obtained fraudulently from victims were **converted into cryptoassets, transferred to another wallet**, and then converted into cash (misuse of a corporate account)

[Illustration of Converting Cryptoassets into Cash via Unlicensed Cryptoasset Broker]*

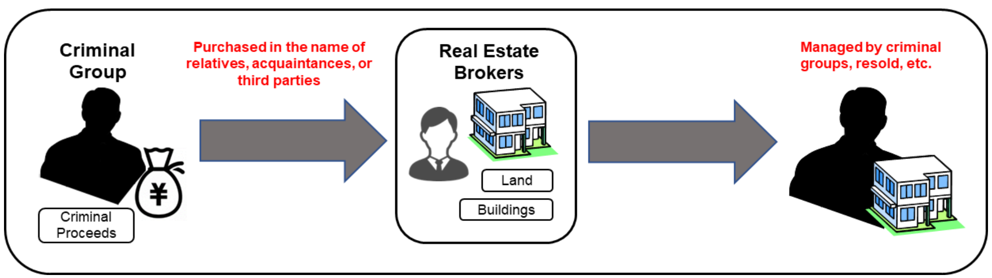


→ A case in which cash derived from criminal proceeds was converted into cryptoassets, transferred through multiple cryptoasset wallets, and then **converted back into cash via unlicensed cryptoasset brokers**

*Unlicensed cryptoasset broker: A party that conducts transactions directly between seller and buyer, setting the price, quantity, and other terms themselves, without going through a stock exchange or other market.
*This table is taken from "Section 4: Risk of Transaction Types, Countries/Regions, and Customer Attributes (p.71)"

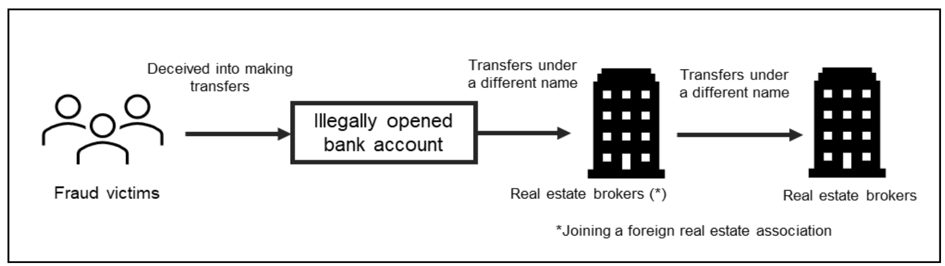
(13) Real Estate Dealt with by Real Estate Brokers (P.188)

[Illustration of ML Using Real Estate Brokers]



→ A case in which the **criminal proceeds were used** to **purchase land and buildings** in the names of relatives, acquaintances, or third parties

[A Case in Which The Proceeds of Online and Telephone Fraud were Transferred to a Real Estate Brokers via a bank account]



→ A case in which the **funds obtained from online and telephone fraud** were sent through fraudulently opened bank accounts to real estate brokers and were subsequently **suspected of being converted into real estate**

Section 5. Risk of Products and Services (P.118)

(i) Factors that Increase Risks (ii) Trends of STRs **(iii) Measures to Mitigate Risks** (iv) Assessment of Risks

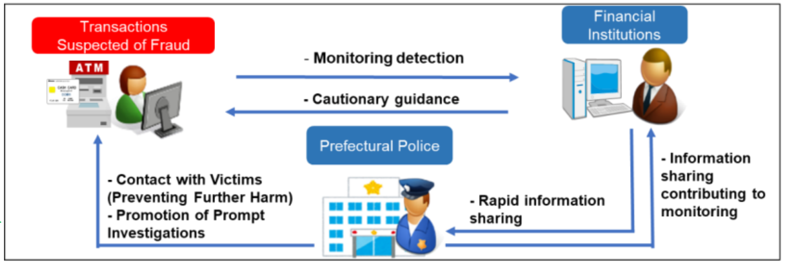
- Between 2024 and 2025, the Financial Services Agency and the National Police Agency jointly, or the National Police Agency alone, have issued the following requests to specified business operators and industry associations.

(1) Products and services dealt with by deposit-taking institutions (P.119)

*Those described in the 2025 NRA-FUR

- In August 2024, it was requested for industry associations to take the various measures to prevent the illicit use of corporate deposit/savings accounts
  In light of the increasingly sophisticated and diverse criminal methods, combined with the misuse of online banking, there have been cases in which funds obtained through online and telephone fraud and similar schemes were transferred to the bank accounts of cryptoassets exchange service providers or funds transfer service providers. Accordingly, in **September 2025**, the authorities issued a request for measures that included the contents of the previous request, as follows:

(1) Strengthening fraud prevention measures and improving understanding of customer circumstances at the time of account opening
(2) Multi-layered detection focusing on appropriateness of user's access environment and the amount and frequency of transactions
(3) Enhancing and refining detection scenarios and thresholds focusing based on the purpose of illicit use and the modus operandi
(4) Expediting detection and subsequent confirmation with customers, as well as measures such as suspension of withdrawals, freezing of accounts, and account closure
(5) Strengthening measures related to online banking
- Verification and warnings at the time of application
- Appropriate setting of initial usage limits
- Verification and warnings after service commencement and when raising usage limits
(6) Suspension of transfers to cryptoassets exchange service providers and funds transfer service providers when the remitter name has been altered
(7) Information sharing between financial institutions that contributes to the detection of signs of illicit use and the understanding of the actual situation
(8) Strengthening information provision and cooperation with the police



- The National Police Agency has concluded "information sharing agreements" with 28 financial institutions (as of the end of September 2025)
- 44 prefectural police have established cooperation with 515 financial institutions (as of the end of June 2025)

- As part of the "measures to deprive criminals of their tools" outlined in the "Comprehensive Measures to Protect People from Frauds" formulated in June 2024, the National Police Agency issued in **December 2024** a notification to the relevant government ministries overseeing financial institutions, requesting that the following specific measures be implemented at each financial institution to prevent the misuse of corporate deposit/savings accounts held in the names of foreigners whose period of stay has expired:
  - When cash withdrawals or transfers to other accounts are made from an account held by a foreigner whose period of stay has expired, conduct verification at the time of transaction to confirm that the account is being used by the account holder in person
  - From the day after the expiration of the residency period, until such verification is completed, restrict cash withdrawals and transfers to other accounts from the relevant account

(3) Products and Services Dealt with by Financial Instruments Business Operators, etc., and Commodity Derivatives Business Operators (P.139)

- Following unauthorized access to online securities accounts, in **July 2025**, requested the entire financial industry to strengthen measures against unauthorized access and fraudulent transactions

(7) Funds Transfer Services Dealt with by Funds Transfer Service Providers (P.157)

- In **September 2025**, requested financial institutions to strengthen measures, including suspending remittances to the bank accounts of funds transfer service providers resulting from changes in the remitter's name

(9) Cryptoassets Dealt with by Cryptoassets Exchange Service Providers (P.166)

- In **September 2025**, requested financial institutions to strengthen measures, including suspending remittances to bank accounts of cryptoasset exchange service providers when the remittance name has been altered

Section 7. Risk Related to Terrorist Financing (P.224)

- From the perspective of clarifying the description of the risks related to terrorist financing, it has been organized as a separate chapter.

Threat	Terrorist organizations, including Islamic extremists such as ISIL and AQ, and those involved in terrorist financing
Vulnerability	Legal and illegal sources and means of terrorist financing

Characteristics of terrorist financing

- **Diversity and concealment of the sources of funds**
  Terrorist financing may be obtained through taxation imposed by terrorist organizations in transactions conducted in regions under their control as well as through activities disguised as legitimate transactions by organizations and companies.
- **Difficulty of detection due to small amount and fragmented transaction types**
  There is a risk that they may become invisible among the numerous transactions handled routinely by business operators
- **Characteristics of the recipient and intermediary locations**
  Money intended for terrorist financing is sent to Iraq, Syria, and Somalia, among others. However, in some cases, money is transferred through Turkey or other neighboring countries
- **Use of Cryptoassets**
  There have been cases where donations in cryptoassets are solicited
- **Use of Social Media**
  The use of social media has been increasing and videos are used to solicit donors
- **Traditional Methods**
  Continue widely using traditional methods, such as hawala and direct cash transfers

Trends in STRs

[Matters to note when submitting STRs]

- **Customer Attributes**
  Verify against the names, dates of birth, and other details of persons subject to asset freezing
- **Countries/Regions Involved in Transaction**
  Whether the countries/regions are where terrorist organizations operate, or a neighboring countries/regions thereof
- **Transaction Types**
  Even if the stated purpose of the remittance is a donation or similar payment, whether the recipient is an organization or individual whose actual activities lack transparency

Assessment of Risk

In Japan, legal measures related to terrorist financing have been established, and compared to other countries, **the risk of terrorist financing is assessed to be relatively low**.
On the other hand, **the following activities should be recognized as concerns:**
- Members of Islamic extremist and other terrorist groups hide themselves in communities of foreigners and misuse the communities
- Foreign fighters engage in revenue-generating activities
- Persons who travel to conflict areas
- Transactions disguised as legitimate ones conducted by Japanese organizations and companies
- Products and services are misused without being monitored by specified business operators

[Topic] Risk of Abuse of Nonprofit Organizations for TF (P.233)

It analyzes the actual conditions and institutional responses for each type of non-profit organization in Japan, and conducts a risk assessment
(1) CESNAs, (2) public interest corporation, (3) social welfare corporation, (4) medical corporation, (5) school corporation, (6) religious corporations , (7) other organizations
→ There have been no cases of nonprofit organizations being prosecuted for being exploited for terrorist financing in Japan and limited number of nonprofit organizations conduct activities abroad. Taking these factors comprehensively, it is considered that they are **at a low risk of terrorist financing** at present

<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