

## **Reference Cases on Suspicious Transactions**

\*Specified business operators other than deposit taking institutions, insurance companies, financial instruments business operators and cryptoasset exchange service providers shall refer to the reference cases for deposit taking institutions, insurance companies, financial instruments business operators and cryptoasset exchange service providers.

(General notes)

The following reference cases are examples of the types of transactions to which financial institutions, etc. should pay special attention as transactions which are likely to fall under suspicious transactions, in performing the obligation to report suspicious transactions as prescribed in Article 8 of the Act on Prevention of Transfer of Criminal Proceeds. Financial institutions, etc. should determine whether or not each individual transaction falls under suspicious transaction by comprehensively taking account of the various specific information they hold with regard to the relevant transaction, such as customer attributes and the circumstances at the time of the transaction while updating such information.

Therefore, it should be noted that: these cases serve as references for financial institutions, etc. to detect or extract suspicious transactions in the course of routine transactions, but transactions that technically correspond to these cases do not necessarily fall under suspicious transactions; and transactions that do not correspond to these cases may be subject to reporting if financial institutions, etc. determine that they fall under suspicious transactions.

### **I. Deposit taking institutions**

#### **No. 1 Cases focused on the pattern of cash usage**

(1) Transactions in which deposits and withdrawals (including the purchase and sale of securities, remittance and money exchange; the same applies hereinafter) are made using large amounts of cash (including foreign currency; the same applies hereinafter) or checks. In particular, large-sum transactions that are inadequate with respect to the customer's attributes, income, assets, past transaction amounts, etc. and transactions in which deposits and withdrawals are made by deliberately using cash despite it being found appropriate to use remittance or bank cashier's checks.

(2) Transactions conducted on a frequent basis in a short period of time, where the total amount of deposits and withdrawals made using cash or checks is large. The same applies to cases where transactions are conducted in an amount slightly below the threshold.

- (3) Transactions in which deposit or money exchange is conducted using large quantities of fractional currency (including foreign currency).
- (4) Transactions related to a deposit of a large amount of cash into a night deposit or a rapid increase in the usage amount in light of the customer's attributes and the business activities, etc.

**No. 2 Cases focused on the possibility of concealing the true account holder**

- (1) Opening of an account under a name suspected to be a fictitious name or another person's name, and deposits and withdrawals using an account that is suspected to have been opened under a fictitious name or another person's name.
- (2) Opening of an account by a legal entity suspected to be a shell company, and deposits and withdrawals using an account whose holder is suspected to be a shell company.
- (3) Deposits and withdrawals using an account related to a customer who requests to have the cash card, etc. sent to a point of contact different from his/her address or who chooses not to receive notices.
- (4) Cases where the same person opens multiple accounts or files applications for purchase using different names (including the same names spelt differently) and different birthdates or otherwise it is suspected that the person is undertaking procedures through impersonation, and cases where it is suspected that a person is applying for the opening of an account or changing the contents of various notifications by pretending to be a third party by sharing or falsifying an identification certificate.
- (5) Cases where a registered email address is the same as one that was found to be suspicious in the past, or cases where an email address used is presumed to be unrelated to the account holder (for example, an address that can be associated with another person or another legal entity) or where email addresses with patterns similar to those of the relevant email address are being used for multiple accounts.
- (6) Cases where the same cell-phone number is registered as the point of contact of multiple accounts or customers.
- (7) Deposits and withdrawals related to a customer who is found to hold multiple accounts

without justifiable grounds. Cases of customers who hold multiple accounts in different names using those containing a trade name, etc., are included.

- (8) Transactions by a person who frequently or in combination changes the person's name, legal entity's name, or sole proprietor' name, and/or the point of contact, telephone number, address, email address, etc.
- (9) Non-face-to-face transactions in which the telephone number, email address, authentication method, etc. are changed at the same time or manipulation by a third party is otherwise suspected.
- (10) Cases where there is no reasonable reason for conducting transactions at the relevant branch in light of the customer's place of residence or place of work, etc.
- (11) Non-face-to-face transactions that are accessed from the same IP address although they are conducted by customers with different names and addresses.
- (12) Non-face-to-face transactions in which the same account is accessed from multiple access environments (multiple IP addresses, devices, etc.).
- (13) Non-face-to-face transactions in which accounts of multiple customers are logged into from the same access environment (the same IP address, device, etc.) and it is suspected that a person related to an online casino is accessing those accounts by pretending to be those customers (online casino users).
- (14) Non-face-to-face transactions for which no rationality can be found in the facts that, although the customer resides in Japan, the IP address used at the time of login is a foreign IP address or that the browser language is a foreign language or no rationality can be found in the inconsistency in the time zones of the device.
- (15) Non-face-to-face transactions in which the tracking of the IP address is made difficult.
- (16) Non-face-to-face transactions for opening an account in which the address obtained upon verification at the time of transaction and the IP address, etc. of the device being used are different.

### **No. 3 Cases focused on the pattern of account usage**

- (1) Transactions related to an account where deposits and withdrawals are made in large amounts or on a frequent basis in a short period of time after opening the account, followed by closing the account or stopping transactions.
- (2) Transactions related to an account in which deposits and withdrawals are frequently made in large amounts in light of the customer' attributes, income, assets, past transaction amounts, etc.
- (3) Transactions related to an account where deposits are frequently made by multiple persons or remittances are frequently made to multiple persons in light of the customer's attributes, income, assets, past transaction amounts, etc. In particular, cases where a remittance is made in large amounts immediately after deposits are made into the account or deposits are made in large amounts into the account immediately before a remittance is made.
- (4) Cases where a transfer or other transaction in a small amount, which is considered to be a test remittance, is completed successfully, and transactions in large amounts are conducted sequentially immediately thereafter.
- (5) Cases where a deposit in a large amount close to the withdrawal limit is made or the balance close to the withdrawal limit is checked, and a withdrawal or a remittance in an amount equal to or slightly below the withdrawal limit is made immediately thereafter.
- (6) Transactions wherein refunding is made in cash from the account immediately followed by remittance of such cash refunded (including cases where such transactions are treated as being made in cash in processing vouchers). In particular, cases where remittance is made by using, as the remitter, a name different from the name of an account to which refunding was made.
- (7) Transactions in which a person attempts to make a remittance by changing the remitter's name to a name different from the name of the account holder. In particular, transactions in which a remittance is to be made to an account at a financial institution held by a cryptoasset exchange service provider (including cases where a transaction has been suspended).

- (8) Transactions related to an account which receives remittance made under anonymity or a name which is presumed to be fictitious.
- (9) Transactions related to an account wherein deposits and withdrawals are abruptly made in large amounts although normally, there are no movements in funds.
- (10) Transactions which are unusual from the viewpoint of economic rationality. For example, cases where the customer refuses high-yielding products without reasonable grounds although a large amount of money is deposited.
- (11) Transactions conducted in unusual patterns or frequency in light of the purpose of transactions, occupation or business verified at the time of opening the account.
- (12) Transactions in which accounts are suspected to be managed by third parties for reasons such that deposits and withdrawals from multiple accounts of different names are frequently made in the same period of time or by using the same ATM, etc.
- (13) Cases where unauthorized use of deposit passbooks, cash cards, debit cards, etc. by third parties is suspected, such that transactions are conducted simultaneously among multiple locations (ATM, etc.) that are difficult to travel to and from in terms of time.
- (14) Transactions wherein the amount of salary paid by bank transfer is unusual in light of the business scale, etc. verified at the time of opening the account.
- (15) Frequent and large-scale transactions by a company established recently or a company that has conducted unusual transactions in light of its business activities, etc.
- (16) Non-face-to-face transactions in which the relevant account is accessed from the same access environment (the same IP address, device, etc.) as an account whose unauthorized use has been identified.
- (17) Non-face-to-face transactions in which transfers are made by an unspecified number of people to an account accessed from the same access environment (the same IP address, device, etc.) as that of a person related to an online casino and to accounts that have had transactions with that account, and it is suspected that collection and payment services in

relation to online casinos are being conducted.

(18) Non-face-to-face transactions in which access inconsistent with information reported by the customer or the customer's past access information is found.

**No. 4 Cases focused on the pattern of purchase and sale of bonds, etc.**

(1) Sale transactions wherein a large volume of bonds, etc. are brought in and are delivered on condition that payment is made in cash.

(2) Transactions wherein purchase and sale of bonds, etc. are settled by checks written by a third party or remittance from a third party.

(3) Transactions related to a customer who does not use the safe custody system and requests delivery of the relevant bond without reasonable grounds, in purchasing large amount of bonds in cash or by checks.

**No. 5 Cases focused on safe custody and safe-deposit box**

(1) The cases prescribed in "No. 2 Cases focused on the possibility of concealing the true account holder" also apply to cases focused on the possibility of concealing the person who is actually conducting transactions related to safe custody or a trust.

(2) The cases prescribed in "No. 2 Cases focused on the possibility of concealing the true account holder" also apply to cases focused on the possibility of concealing the true user of the safe deposit box.

(3) Frequent use of safe-deposit box.

(4) Cases where any suspicious indications regarding a customer are identified when confirming the purpose of use, etc. upon concluding a safe-deposit box agreement or when the customer uses a safe-deposit box.

(5) Cases where it is suspected that a safe-deposit box is used for the purpose of storing goods, etc. (including cash) that is considered to be highly risky from the perspective of preventing money laundering and illegal use, etc. of safe-deposit boxes.

## **No. 6 Cases focused on transactions with foreign countries**

- (1) Transactions related to a customer who provides information suspected to be false or ambiguous information in making remittance to foreign countries (including non-residents of Japan the same applies hereinafter). In particular, transactions related to a customer who provides information which cannot be found to have reasonable grounds with respect to such matters as the recipient, purpose or source of remittance.
- (2) Transactions wherein remittance is frequently made to foreign countries in a short period of time and the total amount of such remittance is large.
- (3) Transactions wherein remittance is made to foreign countries in large amounts for purposes that have no economic rationality.
- (4) Transactions wherein remittance in large amounts that have no economic rationality is received from foreign countries.
- (5) Transactions wherein traveler's checks or emittance checks (including those in foreign currency) are frequently prepared or used in large amounts.
- (6) Transactions related to the issuance of letters of credit in large amounts. In particular, transactions related to a customer who provides information which cannot be found to have reasonable grounds with respect to such matters as the export (producer) country, import volume and import price.
- (7) Transactions conducted by a customer who is based in a country or region that is non-cooperative with measures for anti-money laundering and combating the financing of terrorism ("AML/CFT measures"), or a country or region of export of illicit drugs.
- (8) Transactions conducted by a customer with a person (including a legal entity) who is based in a country or region that is non-cooperative with AML/CFT measures, or a country or region of export of illicit drugs.
- (9) Transactions related to a customer who is possibly related to a person (including a legal entity) who is based in a country or region that is non-cooperative with AML/CFT measures, or a country or region from which illicit drugs are exported.

- (10) Transactions which are suspected of exporting products that do not conform to the technical level of the country of export destination.
- (11) Transactions wherein information such as the name, legal entity name, address and final destination stated in the trade document or transaction telegram is inconsistent.
- (12) Transactions wherein small companies export products with high technical specialties which are unusual in light of their details of business.
- (13) Transactions wherein the descriptions such as the product name made in the trade documents are unspecific.
- (14) Transactions wherein remittance is repeatedly made in small amounts to a person who is presumed to be a relative in a country or region with high risks of human trafficking.

#### **No. 7 Cases focused on loans and repayment thereof**

- (1) Transactions wherein an unscheduled repayment of a delinquent loan is made.
- (2) Application for loans wherein assets held by a third party other than the customer who is the borrower are pledged as collateral.
- (3) Transactions with a customer who is found to have used a loan for a purpose other than the purpose of use reported at the time of loan application.

#### **No. 8 Other cases**

- (1) Cases where public officials or company employees conduct a large-sum transaction that is inadequate with respect to their income.
- (2) Transactions related to multiple stand-alone customers who visit a branch simultaneously and make requests for cash transactions or foreign exchange transactions in large amounts to different tellers.
- (3) Transactions for which verification at the time of transaction cannot be completed due to the customer's uncooperativeness although such transactions had been conducted prior to completion of verification at the time of transaction. For example, cases where documents related to verification at the time of transaction which were to be submitted at

a later date are not submitted. The same applies to cases where an agent is uncooperative.

- (4) Transactions related to a customer who refuses to provide explanation or submit materials although verification of the beneficial owner or other true beneficiary was requested. The same applies to transactions conducted by an agent in which a person other than the customer him/herself is suspected of gaining benefits.
- (5) Transactions wherein the beneficial owner or other true beneficiary of the customer who is a legal entity is likely to be related to criminal proceeds. For example, cases where the beneficial owner is suspected to be a shell company.
- (6) Transactions conducted by the bank's own employee or a person related thereto wherein the person who gains benefits from such transaction is unclear.
- (7) Transactions in which the bank's own employee is suspected of committing crimes prescribed in Article 10 (Concealment of Criminal Proceeds) or Article 11 (Receipt of Criminal Proceeds) of the Act on Punishment of Organized Crimes and Control of Crime Proceeds.
- (8) Transactions wherein deposits are made using counterfeit currency, counterfeit securities, stolen currency or stolen securities and the counterparty to the transaction is suspected of knowing that the relevant currency or securities are those counterfeited or stolen.
- (9) Transactions related to a customer who unnaturally emphasizes the confidentiality of the transaction or a customer who tried requesting, compelling or bribing not to report.
- (10) Transactions related to an organized crime group member or a person related to an organized crime group, and a person who is suspected to be related to a domestic or international criminal organization, etc.
- (11) Transactions conducted in an unusual pattern or those related to a customer who is found to have shown an unusual attitude or movement, etc., in light of the knowledge and experience, etc. of the employee.
- (12) Transactions conducted with a non-profit organization that are found to have no reasonable grounds with respect to the source or final use of funds.

- (13) Transactions wherein remittance is made to a country or region or a third party that is found to have no reasonable relation with the activities of the non-profit organization verified at the time of opening the account.
- (14) Transactions conducted with a foreign politically exposed person ("foreign PEP") that are found to have no reasonable grounds with respect to such matters as the recipient or purpose of remittance.
- (15) Transactions conducted with a foreign PEP that are found to have no reasonable grounds with respect to the assets or source of transactions.
- (16) Transactions conducted with a foreign PEP of a country or region which corruption level is considered high.
- (17) Transactions conducted with a foreign PEP based in a country or region that: has not signed or ratified international conventions related to anti-corruption such as the United Nations Convention against Corruption and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions or is uncooperative with activities based on international conventions related to anti-corruption.
- (18) Cases where an agent is suspected of conducting a transaction to open accounts for the purpose of receiving salary without obtaining the consent from the relevant person him/herself, including transactions conducted with a foreigner such as a technical intern.
- (19) Cases where it is suspected that an account of a foreign national whose period of stay has expired is being used, traded, or otherwise handled through impersonation.
- (20) Transactions for which inquiries or reports have been made from external parties such as public organizations for being likely to be related to criminal proceeds.
- (21) Cases where abnormal conduct (excessively rapid inputs that suggest the possibility of bot control, multiple login failures, etc.) are detected online upon opening or logging into an account online.
- (22) Transactions in which multiple transfers are made under a transerrer's name containing

alphanumeric characters and it is suspected that collection and payment services in relation to online casinos are being conducted.

## **II. Insurance companies**

### **No. 1 Cases focused on the pattern of cash usage**

- (1) Transactions related to a policyholder who pays insurance premiums using large amounts of cash (including foreign currency; the same applies hereinafter) or checks. In particular, cases where large-sum insurance premiums that are inadequate with respect to the policyholder's attributes, income, assets, past transaction amounts, etc. are paid.
- (2) Transactions related to a customer who requests payment be made using cash or checks although the amount of insurance proceeds to be paid or insurance premiums to be refunded is large.
- (3) Payment of insurance premiums made with respect to multiple insurance contracts in a short period of time, where the total amount of payments using cash or checks is large. The same applies to cases where transactions are conducted in an amount slightly below the threshold.
- (4) Transactions in which insurance premiums are paid using a large quantities of fractional currency (including foreign currency).

### **No. 2 Cases focused on the possibility of concealing the true policyholder**

- (1) Conclusion of an insurance contract using a name suspected to be a fictitious name or another person's name, and transactions related to an insurance contract that is suspected to have been concluded using a fictitious name or another person's name.
- (2) Conclusion of an insurance contract by a legal entity suspected to be a shell company, and transactions related to an insurance contract in which the policyholder is suspected to be a shell company.
- (3) Transactions related to a policyholder who requests to have certificates such as insurance policy certificates sent to a point of contact different from his/her address.
- (4) Cases where the same person applies for multiple insurance contracts using different

names (including the same names spelt differently) and different birthdates or otherwise it is suspected that the person is undertaking procedures through impersonation, and cases where it is suspected that a person is applying for an insurance contract or changing the contents of various notifications by pretending to be a third party by sharing or falsifying an identification certificate.

- (5) Cases where a registered email address is the same as one that was found to be suspicious in the past, or cases where an email address used is presumed to be unrelated to the policyholder (for example, an address that can be associated with another person or another legal entity) or where email addresses with patterns similar to those of the relevant email address are being used for multiple accounts.
- (6) Cases where the same cell-phone number is registered as the point of contact of multiple policyholders.
- (7) Transactions related to a policyholder who is found to have concluded multiple insurance contracts without justifiable grounds.
- (8) Transactions by a person who frequently or in combination changes the person's name, legal entity's name, or sole proprietor' name, and/or the point of contact, telephone number, address, email address, etc.
- (9) Non-face-to-face transactions in which the telephone number, email address, authentication method, etc. are changed at the same time or manipulation by a third party is otherwise suspected.
- (10) Transactions related to an offeror who intends to conclude an insurance contract on payment of insurance premiums in large amounts. In particular, cases where the payment method of the insurance premiums is annual payment or lump-sum payment.
- (11) Cases where there is no reasonable reason for conducting transactions at the relevant branch in light of the customer's place of residence or place of work, etc.
- (12) Non-face-to-face transactions that are accessed from the same IP address although they are conducted by policyholders with different names and addresses.

(13) Non-face-to-face transactions for which no rationality can be found in the facts that, although the policyholder resides in Japan, the IP address used at the time of login is a foreign IP address or that the browser language is a foreign language or no rationality can be found in the inconsistency in the time zones of the device.

(14) Non-face-to-face transactions in which the tracking of the IP address is made difficult.

(15) Non-face-to-face transactions in which an application is filed for a contract wherein the address obtained upon verification at the time of transaction and the IP address, etc. of the device being used are different

### **No. 3 Cases focused on the circumstances after the conclusion of contracts**

(1) Transactions which are unusual from the viewpoint of economic rationality. For example, cases where contracts are terminated at an unusually early stage.

(2) Transactions related to a policyholder who abruptly changed the payment method of insurance premiums from monthly payments in small amounts to annual payments or lump-sum payments.

(3) Transactions related to a policyholder who abruptly changed his/her insurance contract to a large-sum insurance where insurance premiums must be paid in large amounts.

(4) Transactions conducted in an unusual pattern or frequency in light of the purpose of transactions, occupation or business verified at the time of conclusion of the contract.

(5) Frequent and large-scale transactions by a company established recently or a company that has conducted unusual transactions in light of its business activities, etc.

(6) Non-face-to-face transactions in which access inconsistent with information reported by the customer or the customer's past access information is found.

(7) Cases where an insurance premium is paid upon conclusion of a contract, and a policyholder terminates the contract immediately thereafter. In particular, cases where, upon a refund of the amount to be appropriated as an insurance premium, a policyholder requests a transfer of that amount to an account held by a person other than the policyholder.

**No. 4 Cases focused on the purchase and sale of bonds, etc.**

- (1) Sale transactions wherein a large volume of bonds, etc. are brought in and are delivered on condition that payment is made in cash.
- (2) Transactions wherein purchase and sale of bonds, etc. are settled by check written by third parties or remittance from third parties.

**No. 5 Cases focused on transactions with foreign countries**

- (1) Transactions related to a beneficiary who requests to receive insurance proceeds or a policyholder who requests to receive refunds in a country or region that is non-cooperative with measures for anti-money laundering and combating the financing of terrorism (“AML/CFT measures”) or a country or region of export of illicit drugs.
- (2) Transactions related to a policyholder who is based in a country or region that is non-cooperative with AML/CFT measures or a country or region of export of illicit drugs.
- (3) Transactions related to a policyholder who is possibly related to a person (including a legal entity) who is based in a country or region that is non-cooperative with AML/CFT measures or a country or region from which illicit drugs are exported.

**No. 6 Cases related to loans**

- (1) Transactions wherein unscheduled repayment of a delinquent loan is made.
- (2) Application for loans wherein assets held by a third party other than the customer who is the counterparty to the loan are pledged as collateral.

**No. 7 Other cases**

- (1) Cases where public officials or company employees pay large-sum insurance premiums that are inadequate with respect to their income.
- (2) Insurance contracts where a company or organization is the policyholder and confirming intention of subscription of each insured is difficult while unusually large-sum insurance premiums are paid or the contract is terminated at an early stage.
- (3) Transactions for which verification at the time of transaction cannot be completed due to

the customer's uncooperativeness although such transactions had been conducted prior to completion of verification at the time of transaction. For example, cases where documents related to verification at the time of transaction which were to be submitted at a later date are not submitted. The same applies to cases where an agent is uncooperative.

- (4) Transactions related to a policyholder who refuses to provide an explanation or submit materials although verification of the beneficial owner or other true beneficiary was requested. The same applies to transactions conducted by an agent in which the other party is suspected of gaining benefits.
- (5) Transactions wherein the beneficial owner or other true beneficiary of the customer who is a legal entity is likely to be related to criminal proceeds. For example, cases where the beneficial owner is suspected to be a shell company.
- (6) Transactions conducted by the insurance company's own employee or a person related thereto wherein the person who gains benefits from such transaction is unclear.
- (7) Transactions in which the insurance company's own employee is suspected of committing crimes prescribed in Article 10 (Concealment of Criminal Proceeds) or Article 11 (Receipt of Criminal Proceeds) of the Act on Punishment of Organized Crimes and Control of Crime Proceeds.
- (8) Transactions wherein deposits are made using counterfeit currency, counterfeit securities, stolen currency or stolen securities and the counterparty to the transaction is suspected of knowing that the relevant currency or securities are those counterfeited or stolen.
- (9) Transactions related to a customer who unnaturally emphasizes the confidentiality of the transaction or a customer who tried requesting, compelling or bribing not to report.
- (10) Transactions related to an organized crime group member or person related to an organized crime group, and a person who is suspected to be related to a domestic or international criminal organization, etc.
- (11) Transactions conducted in an unusual pattern or those related to a policyholder who is found to have shown an unusual attitude or movement, etc., in light of the knowledge and experience, etc. of the employee.

- (12) Transactions conducted with a non-profit organization that are found to have no reasonable grounds with respect to the source or final use of funds.
- (13) Transactions related to a country or region or a third party that is found to have no reasonable relation with the activities of the non-profit organization verified at the time of conclusion of the contract.
- (14) Transactions conducted with a foreign politically exposed person ("foreign PEP") that are found to have no reasonable grounds with respect to such matters as the purpose of transaction.
- (15) Transactions conducted with a foreign PEP that are found to have no reasonable grounds with respect to the assets or source of transactions.
- (16) Transactions conducted with a foreign PEP of a country or region which corruption level is considered high.
- (17) Transactions conducted with a foreign PEP based in a country or region that: has not signed or ratified international conventions related to anti-corruption such as the United Nations Convention against Corruption and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions or is uncooperative with activities based on international conventions related to anti-corruption.
- (18) Transactions for which inquiries or reports have been made from external parties such as public organizations for being likely to be related to criminal proceeds.
- (19) Cases where abnormal conduct (excessively rapid inputs that suggest the possibility of bot control, multiple login failures, etc.) are detected online upon logging into an account, etc.

Others

### **III. Financial instruments business operators**

#### **No. 1 Cases focused on the pattern of cash usage**

- (1) Transactions in which investments in stocks, bonds, investment trusts, etc. are made using large amounts of cash (including foreign currency; the same applies hereinafter) or checks. In particular, large-sum transactions that are inadequate with respect to the customer's attributes, income, assets, past transaction amounts, etc.
- (2) Investments made in stocks, bonds or investment trusts, etc. on a frequent basis in a short period of time, where the total amount of transactions conducted using cash or checks is large. The same applies to cases where transactions are conducted in an amount slightly below the threshold.
- (3) Transactions in which investments in stocks, bonds or investment trusts, etc. are made using large quantities of fractional currency (including foreign currency).

**No. 2 Cases focused on the possibility of concealing the person who is actually conducting transaction**

- (1) Opening of an account under a name suspected to be a fictitious name or another person's name, and investments in stocks, bonds, investment trusts, etc. using an account that is suspected to have been opened under a fictitious name or another person's name.
- (2) Opening of an account by a legal entity suspected to be a shell company, and investments in stocks, bonds, investment trusts, etc. using an account whose holder is suspected to be a shell company.
- (3) Investments in stocks, bonds or investment trusts, etc. using an account related to a customer who requests to have documents such as transaction reports sent to a point of contact different from his/her address.
- (4) Cases where the same person opens multiple accounts or files applications for purchase using different names (including the same names spelt differently) and different birthdates or it is otherwise suspected that the person is undertaking procedures, etc. through impersonation, and cases where it is suspected that a person is applying for the opening of an account or changing the contents of various notifications by pretending to be a third party by sharing or falsifying an identification certificate.
- (5) Cases where a registered email address is the same as one that was found to be suspicious in the past, or cases where an email address used is presumed to be unrelated

to the account holder (for example, an address that can be associated with another person or another legal entity) or where email addresses with patterns similar to those of the relevant email address are being used for multiple accounts.

- (6) Cases where the same cell-phone number is registered as the point of contact of multiple accounts or customers.
- (7) Investments in stocks, bonds or investment trusts, etc. related to a customer who is found to hold multiple accounts without justifiable grounds.
- (8) Transactions by a person who frequently or in combination changes the person's name, legal entity's name, or sole proprietor' name, and/or the point of contact, telephone number, address, email address, etc.
- (9) Non-face-to-face transactions in which the telephone number, email address, authentication method, etc. are changed at the same time or manipulation by a third party is otherwise suspected.
- (10) Cases where there is no reasonable reason for conducting transactions at the relevant branch in light of a customer's place of residence or place of work, etc.
- (11) Non-face-to-face transactions that are accessed from the same IP address although they are conducted by customers with different names and addresses.
- (12) Non-face-to-face transactions in which the same account is accessed from multiple access environments (multiple IP addresses, devices, etc.).
- (13) Non-face-to-face transactions for which no rationality can be found in the facts that, although the customer resides in Japan, the IP address used at the time of login is a foreign IP address or that the browser language is a foreign language or no rationality can be found in the inconsistency in the time zones of the device.
- (14) Non-face-to-face transactions in which the tracking of the IP address is made difficult.
- (15) Non-face-to-face transactions for opening an account in which the address obtained upon verification at the time of transaction and the IP address, etc. of the device being

used are different.

### **No. 3 Cases focused on the pattern of investment**

- (1) Transactions related to an account wherein investments are abruptly made in large amounts although normally, no transactions are conducted.
- (2) Transactions related to deposit (transfer) of a large volume of the customer's own stocks or another person's stocks from other securities companies, etc. without reasonable grounds.
- (3) Transactions wherein stocks are deposited (transferred) from other securities companies, etc. and are sold and withdrawn (transferred) in a repetitive manner on a frequent basis without reasonable grounds.
- (4) Transactions wherein settlement is made using checks written by a third party or remittance from a third party.
- (5) Transactions conducted in unusual patterns or frequencies in light of the purpose of transactions, occupation or business verified at the time of conclusion of contract.
- (6) Cases where unauthorized use of cash cards, etc. by third parties is suspected, such that transactions are conducted simultaneously among multiple locations (ATM, etc.) that are difficult to travel to and from in terms of time.
- (7) Non-face-to-face transactions in which the relevant account is accessed from the same access environment (the same IP address, device, etc.) as an account whose unauthorized use has been identified.
- (8) Non-face-to-face transactions in which access inconsistent with information reported by the customer or the customer's past access information is found.

### **No. 4 Cases related to safe custody**

- (1) The cases prescribed in "No. 2 Cases focused on the possibility of concealing the person who is actually conducting transaction" also apply to cases focused on such matters as the circumstances at the time of conclusion of the safe custody contract.

- (2) Transactions related to a customer who transfers stocks or bonds in large amounts to other securities companies, etc. without reasonable grounds after purchasing them.

**No. 5 Cases focused on transactions with foreign countries**

- (1) Transactions related to a customer who is based in a country or region that is non-cooperative with measures for anti-money laundering and combating the financing of terrorism (“AML/CFT measures”) or a country or region of export of illicit drugs.
- (2) Transactions related to a customer who intends to designate a bank account based in a county or region that is non-cooperative with AML/CFT measures or a country or region of export of illicit drugs, as the bank account for transfer of sales proceeds.
- (3) Transactions related to a customer who is possibly related to a person (including a legal entity) who is based in a country or region that is non-cooperative with AML/CFT measures, or a country or region from which illicit drugs are exported.

**No. 6 Cases focused on business related to issuance of securities**

- (1) Issuance of securities by a company which is suspected to have persons involved in management separately from the nominal manager.
- (2) Issuance of securities with respect to which an organized crime group member or person related to an organized crime group, and a person who is suspected to be related to a domestic or international criminal organization, etc. is suspected to be involved in any of such persons concerned as the major shareholder, officer, standing proxy, major creditor, major trading partner, or arranger.
- (3) Issuance of securities by a company whose relation between the usage of funds it intends to procure from the issuance of securities and its businesses is unusual.
- (4) Issuance of securities by a company for which there are doubts, such that the change in business activities or establishment of new business made after the previous issuance of securities is found to have no relation with the company’s previous businesses.
- (5) Issuance of securities which will result in a significant (extreme) scale of capital increase in comparison to the number of issued stocks, net sales and assets, etc. prior to the capital

increase.

- (6) Issuance of securities in significant amounts that is repeatedly made in a short period of time, contrary to the business activities, size, etc. of the issuing entity.
- (7) Issuance of securities by a company wherein officers or financial auditors are frequently replaced or wherein resignation or removal of officers or financial auditors is made in an unusual manner.
- (8) Issuance of securities through such means as capital increase by way of third party allotment of stocks wherein a fund, etc. which is registered or based in a country or region that is noncooperative with AML/CFT measures, or a country or region of export of illicit drugs is the allottee.
- (9) Issuance of securities through such means as capital increase by way of third party allotment of stocks wherein a fund, etc. whose substantial investor, underwriting funds and other economic reality remain unclear is the allottee.
- (10) Issuance of securities through such means as capital increase by way of third party allotment of stocks wherein, superficially, there are multiple allottees, but in reality, the persons or funds, etc. that are suspected to be substantially the same is the allottee.
- (11) Act of depositing a large volume of securities wherein an investment partnership is a third party allottee.

#### **No. 7 Other cases**

- (1) Cases where public officials or company employees conduct a large-sum transaction that is inadequate with respect to their income.
- (2) Transactions for which verification at the time of transaction cannot be completed due to the customer's uncooperativeness although such transactions had been conducted prior to completion of verification at the time of transaction. For example, cases where documents related to verification at the time of transaction which were to be submitted at a later date are not submitted. The same applies to cases where an agent is uncooperative.
- (3) Transactions related to a customer who refuses to provide an explanation or submit

materials although verification of the beneficial owner or other true beneficiary was requested. The same applies to transactions conducted by an agent in which a person other than the customer him/herself is suspected of gaining benefits.

- (4) Transactions wherein the beneficial owner or other true beneficiary of the customer who is a legal entity is likely to be related to criminal proceeds. For example, cases where the beneficial owner is suspected to be a shell company.
- (5) Transactions conducted by the financial instruments business operator's own employee or a person related thereto wherein the person who gains benefits from such transaction is unclear.
- (6) Transactions in which the financial instruments business operator's own employee is suspected of committing crimes prescribed in Article 10(Concealment of Criminal Proceeds) or Article 11(Receipt of Criminal Proceeds) of the Act on Punishment of Organized Crimes and Control of Crime Proceeds.
- (7) Transactions wherein deposits are made using counterfeit currency, counterfeit securities, stolen currency or stolen securities and the counterparty to the transaction is suspected of knowing that the relevant currency or securities are those counterfeited or stolen.
- (8) Transactions related to a customer who unnaturally emphasizes the confidentiality of the transaction or a customer who tried requesting, compelling or bribing not to report.
- (9) Transactions related to an organized crime group member or person related to an organized crime group, and a person who is suspected to be related to a domestic or international criminal organization, etc.
- (10) Transactions conducted in an unusual pattern or those related to a customer who is found to have shown an unusual attitude or movement, etc., in light of the knowledge and experience, etc. of the employee.
- (11) Transactions conducted with a non-profit organization that are found to have no reasonable grounds with respect to the source or final use of funds.
- (12) Investments made in a country or region or a third party that is found to have no

reasonable relation with the activities of the non-profit organization verified at the time of opening the account.

(13) Transactions conducted with a foreign politically exposed person ("foreign PEP") that are found to have no reasonable grounds with respect to such matters as the purpose of transactions.

(14) Transactions conducted with a foreign PEP that are found to have no reasonable grounds with respect to the assets or source of transactions.

(15) Transactions conducted with a foreign PEP of a country or region which corruption level is considered high.

(16) Transactions conducted with a foreign PEP based in a country or region that: has not signed or ratified international conventions related to anti-corruption such as the United Nations Convention against Corruption and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions or is uncooperative with activities based on international conventions related to anti-corruption.

(17) Transactions for which inquiries or reports have been made from external parties such as public organizations for being likely to be related to criminal proceeds.

(18) Cases where abnormal conduct (excessively rapid inputs that suggest the possibility of bot control, multiple login failures, etc.) are detected online upon opening or logging into an account online.

Others

#### **IV. Cryptoasset exchange service providers**

##### **No. 1 Cases focused on the pattern of cash usage**

(1) Transactions in which the purchase and sale of cryptoassets is conducted using large amounts of cash (including foreign currency; the same applies hereinafter). In particular, large-sum transactions that are inadequate with respect to the customer's attributes, income, assets, past transaction amounts, etc. and transactions in which the purchase and sale of cryptoassets is conducted by deliberately using cash even in cases where it is

found appropriate to use remittance.

- (2) Transactions conducted on a frequent basis in a short period of time, where the total amount of purchase and sale of cryptoassets conducted using cash is large. The same applies to cases where transactions are conducted in amounts lightly below the threshold.
- (3) Transactions in which purchase of cryptoassets is conducted using large quantities of fractional currency (including foreign currency).

**No. 2 Cases focused on the possibility of concealing the true account holder**

- (1) Opening of an account under a name suspected to be a fictitious name or another person's name, and deposits and withdrawals of money or cryptoassets, purchase and sale of cryptoassets, or exchange with other cryptoassets using an account that is suspected to have been opened under a fictitious name or another person's name.
- (2) Opening of an account by a legal entity suspected to be a shell company, and deposits and withdrawals of money or cryptoassets, purchase and sale of cryptoassets, or exchange with other cryptoassets using an account whose holder is suspected to be a shell company.
- (3) Deposits and withdrawals of cryptoassets, purchase and sale of cryptoassets, or exchange with other cryptoassets using an account related to a customer who requests to have the transaction documents, etc. sent to a point of contact different from his/her address or who chooses not to receive notices.
- (4) Cases where the same person opens multiple accounts or files applications for purchase using different names (including the same names spelt differently) and different birthdates or it is otherwise suspected that the person is undertaking procedures, etc. through impersonation, and cases where it is suspected that a person is applying for the opening of an account or changing the contents of various notifications by pretending to be a third party by sharing or falsifying an identification certificate.
- (5) Cases where a registered email address is the same as one that was found to be suspicious in the past, or cases where an email address used is presumed to be unrelated to the account holder (for example, an address that can be associated with another person

or another legal entity) or where email addresses with patterns similar to those of the relevant email address are being used for multiple accounts.

(6) Cases where the same cell-phone number is registered as the point of contact of multiple accounts or customers.

(7) Deposits and withdrawals of money or cryptoassets, purchase and sale of cryptoassets or exchange with other cryptoassets related to a customer who is found to hold multiple accounts without justifiable grounds. Cases of customers who hold multiple accounts in different names using those containing a trade name, etc. are included.

(8) Transactions by a person who frequently or in combination changes the person's name, legal entity's name, or sole proprietor' name, and/or the point of contact, telephone number, address, email address, etc.

(9) Non-face-to-face transactions in which the telephone number, email address, authentication method, etc. are changed at the same time or manipulation by a third party is otherwise suspected.

(10) Deposits and withdrawals of money or cryptoassets, purchase and sale of cryptoassets or exchange with other cryptoassets by a customer who has no clear reason for conducting face-to-face transactions with the relevant service provider or conducting transactions using the relevant automatic cryptoasset exchange machine.

(11) Cases where a customer deposits cryptoassets via a tool that makes the tracking of transactions difficult (a transaction mixer, tumbler, bridge, etc.) and cases where a customer deposits cryptoassets to such a tool or uses such a tool after depositing cryptoassets.

(12) Non-face-to-face transactions that are accessed from the same IP address although they are conducted by customers with different names and addresses.

(13) Non-face-to-face transactions in which the same account is accessed from multiple access environments (multiple IP addresses, devices, etc.).

(14) Non-face-to-face transactions for which no rationality can be found in the facts that,

although the customer resides in Japan, the IP address used at the time of login is a foreign IP address or that the browser language is a foreign language or no rationality can be found in the inconsistency in the time zones of the device.

(15) Non-face-to-face transactions in which the tracking of the IP address is made difficult.

(16) Non-face-to-face transactions in which an account is opened while the address obtained upon verification at the time of transaction and the IP address, etc. of the device being used are different.

### **No. 3 Cases focused on the pattern of account usage**

(1) Transactions related to an account in which deposits and withdrawals of money or cryptoassets are made in large amounts or on a frequent basis in a short period of time after opening the account, followed by the closing of the relevant account.

(2) Transactions related to an account in which deposits and withdrawals of money or cryptoassets are frequently made in large amounts in light of the customer's attributes, income, assets, past transaction amounts, etc.

(3) Transactions related to an account in which cryptoassets are frequently deposited from multiple addresses or are frequently withdrawn from the account to multiple addresses in light of the customer's attributes, income, assets, past transaction amounts, etc. In particular, cases where a withdrawal of cryptoassets or money is made in large amounts immediately after the cryptoassets are deposited into the account or cryptoassets or money is deposited in large amounts immediately before the withdrawal of cryptoassets is made.

(4) Cases where a transaction in a small amount is completed successfully, and transactions in large amounts are conducted sequentially immediately thereafter.

(5) Deposits of money wherein the transferrer's name was changed to a name different from the name of the account holder, or withdrawal of money to an account under a name different from the name of the account holder.

(6) Transactions related to an account from which withdrawals of cryptoassets are made under anonymity or a name that is presumed to be fictitious.

- (7) Cases where deposits and withdrawals of cryptoassets are abruptly made in large amounts although normally there are no transactions.
- (8) Transactions conducted in unusual patterns or frequency in light of the purpose of transactions, occupation, or business, etc. verified at the time of opening the account.
- (9) Frequent and large-scale transactions by a company established recently or a company that has conducted unusual transactions in light of its business activities, etc.
- (10) Non-face-to-face transactions in which the relevant account is accessed from the same access environment (the same IP address, device, etc.) as an account whose unauthorized use has been identified.
- (11) Non-face-to-face transactions in which access inconsistent with information reported by the customer or the customer's past access information is found.
- (12) Cases where an address used by a customer as the address for deposit or withdrawal of cryptoassets is the same as or is related to one that was found to be suspicious in the past.

#### **No. 4 Cases focused on the pattern of transaction**

- (1) Sale transaction wherein cryptoassets are delivered on condition that payment is made in cash, conducted on a frequent basis in a short period of time.
- (2) Transactions related to a customer who intends to designate a bank account held under the name of a third party as the bank account for deposit of money or transfer of sales proceeds.

#### **No. 5 Cases focused on transactions with foreign countries**

- (1) Transactions related to a customer who is based in a country or region that is non-cooperative with measures for anti-money laundering and combating the financing of terrorism ("AML/CFT measures") or a country or region of export of illicit drugs.
- (2) Transactions related to a customer who intends to designate a bank account based in a country or region that is non-cooperative with AML/CFT measures or a country or region

of export of illicit drugs as the bank account for deposit of money or transfer of sales proceeds.

(3) Transactions related to a customer who may be related to a person (including a legal entity) who is based in a country or region that is non-cooperative with AML/CFT measures or a country or region from which illicit drugs are exported.

#### **No. 6 Other cases**

(1) Cases where public officials or company employees conduct a large-sum transaction that is inadequate with respect to their income.

(2) Cases where transactions are conducted in such manner that the amount of purchase and sale of cryptoassets per person slightly falls below the amount (stipulated by law or the service provider's own rules) that would be subject to verification at the time of transaction.

(3) Cases where the same customer visits the same or nearby branch or automatic cryptoasset exchange machine on the same day or days in close proximity several times and conducts transactions in such manner that the amount of transaction falls slightly below the amount (stipulated by law or the service provider's own rules) that would be subject to verification at the time of transaction.

(4) Transactions for which verification at the time of transaction cannot be completed due to the customer's uncooperativeness although such transactions had been conducted prior to completion of verification at the time of transaction. For example, cases where documents related to verification at the time of transaction which were to be submitted at a later date are not submitted. The same applies to cases where an agent is uncooperative.

(5) Transactions related to a customer who refuses to provide an explanation or submit materials although verification of the beneficial owner or other true beneficiary was requested. The same applies to transactions conducted by an agent in which a person other than the customer him/herself is suspected of gaining benefits.

(6) Transactions wherein the beneficial owner or other true beneficiary of the customer who is a legal entity is likely to be related to criminal proceeds. For example, cases where the beneficial owner is suspected to be a shell company.

- (7) Transactions conducted by the cryptoasset exchange service provider's own employee or a person related thereto wherein the person who gains benefits from such transaction is unclear.
- (8) Transactions in which the cryptoasset exchange service provider's own employee is suspected of committing crimes prescribed in Article 10 (Concealment of Criminal Proceeds) or Article 11 (Receipt of Criminal Proceeds) of the Act on Punishment of Organized Crimes and Control of Crime Proceeds.
- (9) Transactions wherein deposits are made using counterfeit currency, stolen currency, or stolen cryptoassets and the counterparty to the transaction is suspected of knowing that the relevant currency is counterfeit or stolen or that the relevant cryptoassets are stolen.
- (10) Transactions related to a customer who unnaturally emphasizes the confidentiality of the transaction or a customer who tried requesting, compelling or bribing not to report.
- (11) Transactions related to an organized crime group member or person related to an organized crime group, and a person who is suspected to be related to a domestic or international criminal organization, etc.
- (12) Transactions conducted in an unusual pattern or those related to a customer who is found to have shown an unusual attitude or movement, etc., in light of the knowledge and experience, etc. of the employee.
- (13) Transactions conducted with a non-profit organization that are found to have no reasonable grounds with respect to the source or final use of funds.
- (14) Transactions related to a country or region or a third party that is found to have no reasonable relation to the activities, etc. of the non-profit organization verified at the time of opening the account.
- (15) Transactions conducted with a foreign politically exposed person ("foreign PEP") that are found to have no reasonable grounds with respect to such matters as the purpose of transactions.

- (16) Transactions conducted with a foreign PEP that are found to have no reasonable grounds with respect to the assets or source of transactions.
- (17) Transactions conducted with a foreign PEP of a country or region which corruption level is considered high.
- (18) Transactions conducted with a foreign PEP based in a country or region that: has not signed or ratified international conventions related to anti-corruption such as the United Nations Convention against Corruption and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions or is uncooperative with activities based on international conventions related to anti-corruption.
- (19) Cases where another address, which is suspected to have a strong relation to the address used by a customer as the address for deposit or withdrawal of cryptoassets due to facts such that transactions are conducted on a frequent basis between such addresses, is used for cryptoasset transactions while using anonymization techniques.
- (20) Transactions with a customer who has an address that receives deposits of cryptoassets from multiple addresses or withdraws cryptoassets to multiple addresses on the blockchain.
- (21) Transactions for which inquiries or reports have been made from outsiders such as public organizations for being likely to be related to criminal proceeds.
- (22) Cases where unusual conduct (excessively rapid inputs that suggest the possibility of bot control, multiple login failures, etc.) are detected online upon opening or logging into an account.
- (23) Transactions in which cryptoassets are sent and received in large amounts, or high frequency, or at considerably low prices to and from addresses relating to a dark net marketplace, a ransomware group, an online casino website, etc.
- (24) Transactions in which there are no materials to prove the source of the cryptoassets or the funds converted to cryptoassets.
- (25) Transactions to transfer cryptoassets to a cryptoasset wallet that has a connection with illegal acts on the dark web.

(26) Suspicious transactions relating to a P2P wallet, such as those in which money deposited to an account is immediately exchanged with cryptoassets and the cryptoassets are withdrawn to a P2P wallet or in which cryptoassets deposited from a P2P wallet are immediately converted to cash.

Others

#### **V. Certified Public Accountants, etc.**

(General notes)

The following reference cases are examples of the types of transactions to which certified public accountants and audit corporations (hereinafter referred to as "certified public accountants, etc.") should pay special attention as transactions that are likely to fall under suspicious transactions, in performing the obligation to report suspicious transactions as prescribed in Article 8, paragraph (2) of the Act on Prevention of Transfer of Criminal Proceeds. Certified public accountants, etc. should determine whether or not each individual transaction falls under a suspicious transaction by comprehensively taking account of the various specific information they hold with regard to the relevant transaction, such as customer attributes and the circumstances at the time of the transaction.

Therefore, it should be noted that: these cases serve as references for certified public accountants, etc. to detect or extract suspicious transactions in the course of routine transactions, but transactions that technically correspond to these cases do not necessarily fall under suspicious transactions, such as in cases where there are reasonable grounds, etc.; and transactions that do not correspond to these cases may be subject to reporting if certified public accountants, etc. determine that they fall under suspicious transactions.

#### **No. 1 Cases involving the agency or proxy of acts or procedures related to the sale or purchase of residential land or buildings for the benefit of customers**

(1) Cases where residential land or buildings are purchased using large amounts of cash (in particular, cases in which the purchase is an expensive property that is not commensurate with the customer's attributes, such as income and assets).

(2) Cases where the same person purchases or sells a large number of residential land or buildings within a short period of time.

- (3) Cases where residential land or a residential building is purchased and then sold within a short period of time.
- (4) Cases where a transaction is unusual from the viewpoint of economic rationality (for example, cases where a customer rushes to sell and is willing to sell at a price well below the market price).
- (5) Cases where a customer purchases multiple properties within a short period of time but shows little concern about the location, condition, or expected repair costs of each property.
- (6) Cases where no reasonable grounds can be found for a customer to purchase or sell the land or building that is the subject of the transaction, in light of the scale of the transaction, the location of the property, or the nature of the customer's business.
- (7) Cases where the legal entity that is the contracting party of a sales contract is suspected to be a shell company.

**No. 2 Cases involving the agency or representation of acts or procedures related to the establishment or merger of a company for the benefit of customers**

- (1) Cases where no reasonable grounds can be found for establishing a company, such as establishing a legal entity with no specific prospects for its activity.
- (2) Cases where multiple companies are being established within a short period of time without reasonable grounds.
- (3) Cases where the representative of a legal entity is a foreign national and the representative's status of residence has restrictions on work.
- (4) Cases where the number of business objectives is diverse without any reasonable grounds and they are poorly related to each other.
- (5) Cases where clear responses cannot be obtained when asking for an explanation of the business activities, etc.
- (6) Cases where a large number of legal entities are to be established at the same address without reasonable grounds.

- (7) Cases where a legal entity is to be established whose business details are activities in areas where terrorist acts are being carried out or in the surrounding area, without reasonable grounds.

**No. 3 Cases involving the agency or representation of the management or disposal of cash, deposits, securities, or other property for the benefit of customers**

- (1) Cases where the account of certified public accountants, etc. is to be used for the storage of funds, etc.

**No. 4 Cases focused on the possibility of concealing the true contractor**

- (1) Cases where a contract is suspected to have been concluded using a fictitious name or another person's name.
- (2) Cases where a customer refuses to write his/her name on the relevant transaction documents or to present identity verification documents.
- (3) Cases where identity verification documents presented by a customer during identity verification are suspected of being forged.
- (4) Cases where a customer intends to use a different name on each of the relevant transaction documents.
- (5) Cases where a person related to a legal entity that is suspected to be a shell company is involved in the transaction.
- (6) Cases where a customer requests that relevant documents be sent to a contact address that is different from the customer's address.

**No. 5 Cases focused on transactions with foreign countries**

- (1) Transactions conducted by a customer who is based in a country or region that is non-cooperative with measures for anti-money laundering and combating the financing of terrorism ("AML/CFT measures") or a country or region of export of illicit drugs.
- (2) Transactions related to a customer introduced by a person (including a legal entity) who is based in a country or region that is non-cooperative with AML/CFT measures, or a

country or region of export of illicit drugs.

#### **No. 6 Other cases**

- (1) Cases where public officials or company employees conduct a large-sum transaction that is not commensurate with their income.
- (2) Cases where a customer refuses to provide an explanation or submit materials even though verification of the true beneficiary was requested due to suspicion as to whether or not the customer is acting for him/herself.
- (3) Cases where a customer unnaturally emphasizes the confidentiality of the transaction.
- (4) Cases where a customer tries requesting, compelling, or bribing to prevent the filing of a suspicious transaction report.
- (5) Transactions related to an organized crime group member or a person related to an organized crime group.
- (6) Transactions conducted in an unusual pattern or those related to a customer who is found to have shown an unusual attitude or movement, etc., in light of the knowledge and experience of the certified public accountants, etc.
- (7) Transactions conducted with a foreign PEP of a country or region with a high level of corruption.
- (8) Transactions for which inquiries or reports have been made from external parties, such as public organizations, due to the likelihood of being related to criminal proceeds.

Others