※As of June 2021

5. Guidelines for Supervision of Issuers of Prepaid Payment Instruments（Provisional Translation）

I. General

I-1 Scope, etc. of Prepaid Payment Instruments

If an inquiry, etc. is received with regard to the scope, etc. of Prepaid Payment Instruments prescribed in the Payment Services Act (Act No. 59 of 2009, hereinafter referred to as the "Act"), the scope shall be determined as follows.

I-1-1 Certificates, etc., or numbers, markings, or other symbols that do not fall under the category of Prepaid Payment Instruments

(1) Certificates, etc. or numbers, markings, or other symbols listed below do not fall under the category of Prepaid Payment Instruments prescribed in Article 3 (1) of the Act.

(i) "Bank of Japan notes", "fiscal stamps", "postage stamps", "stamps," etc., which are given the effect of valuables by laws;

(ii) Various memberships (limited to those that have the nature of evidence certificate) such as "golf club membership certificate" and "tennis club membership certificate";

(iii) "Trading stamps," etc., that are sold to a person who uses them only in a commercial transaction and that the purchaser does not plan to resell to consumers;

(iv) POS-type cards using magnetic cards or IC cards; or

(v) Items that serve as means of identification, etc., whose certificates, etc., or numbers, markings, or other symbols themselves are not valuable and that have no connection with the property value recorded on the certificate, etc., an electronic device, or any other object.

Note: "Items that serve as means of identification, etc., whose certificates, etc., or numbers, markings, or other symbols themselves are not valuable and that have no connection with the property value recorded on the certificate, etc., an electronic device or any other object" refers to items that satisfy both of the following requirements (A) and (B).

(A) A user is limited to the right holder by signature, personal identification number, etc.

(B) Even when a user does not use the certificates, etc., or numbers, markings, or other symbols, if the issuer confirms that the user is the right holder in certain means, the user is able to purchase goods or use service, etc., and all of the requirements set forth in i) through iii) below are satisfied.

i) The unused balance and the used balance are able to be managed via books or other means without relying on the certificates, etc., or numbers, markings, or other symbols.

ii) A system is in place whereby even when a user does not use the certificates, etc., numbers, markings, or other symbols, if the issuer confirms that the user is the right holder in certain means, the user is able to purchase goods or use services, etc., and such system is actually operated for users in general.

iii) With regard to such certificates, etc., numbers, markings, or other symbols, no indication or explanation is given that would mislead users to consider it as "Prepaid Payment Instruments" such as "Users are able to exercise their rights by presenting the certificates, etc., or numbers, markings, or other symbols".

(vi) Certificates, etc., or numbers, markings, or other symbols whose property value stated or recorded on the certificates, etc. will not decrease with the use of such certificates, etc., or numbers, markings, or other symbols.

(2) With regard to certificates, etc., or numbers, markings, or other symbols for which refunds (conversion into cash or withdraws of cash) are permitted beyond the cases prescribed in Article 20(1) or (5) of the Act, it should be kept in mind that issuers thereof are not able to make a notification or registration as an Issuer of Prepaid Payment Instruments, because these kind of certificates, etc., or numbers, markings, or other symbols are different in nature from the Prepaid Payment Instruments.

I-1-2 Close Relationship with Issuer

The term "the relationship between an issuer and the person that simultaneously or continuously carries on delivery of goods or provision of services that are closely related with and inseparable from delivery of goods or provision of services carried on by the issuer, if the relevant person exists" prescribed in Article 3(1)(v) of the Order for Enforcement of the Payment Services Act (Cabinet Order No. 19 of 2010, hereinafter referred to as the "Order") means a relationship in which the delivery of goods or provision of services by the relevant party is indispensable for the issuer to deliver goods or provide services and in which both are considered to be an integral part in general societal terms, and does not include a mere business alliance.

I-1-3 Prepaid Payment Instruments Excluded from Application of the Act

The "Exclusion from Application" under Article 4 of the Act shall be treated as follows.

(1) The "date of issuance" prescribed in Article 4(ii) of the Act means the date listed in the following, whichever is later;
   (i) the date when the property value is stated or recorded on the certificates, etc., an electronic device, or any other object; or
   (ii) the date when the certificates, etc., or numbers, markings, or other symbols are issued or granted to a user.

(2) The provision of Article 4(1)(iii) of the Order shall be construed as follows.
   (i) The term "issued in conjunction with the use of" means the case where only the portion necessary for the use is issued and purchased every time it is used or just before the use, and basically there is no remaining balance after the use.
   (ii) The term "that are designed to be used normally by the users" means the case where the users cannot be provided with services or goods, in principle, without such certificates, etc.

(3) Pursuant to Article 4(1)(iv) of the Order, among Server-type Prepaid Payment Instruments, those that are confirmed to have a function equivalent to the certificates, etc. listed in the (i) through (iii) of the same paragraph are not subject to application of the Act.
   However, when goods and services are provided solely through the Internet, for example, cases where the process of accessing a virtual space on the Internet is referred to as an "admission ticket" or where services provided in a virtual space are referred to as a "passenger ticket" or a "meal ticket", such cases are subject to the Act because they fall under the provision in the parentheses in the same item.
   Note: The term "Server-type Prepaid Payment Instrument" as used in these Guidelines means, among the Prepaid Payment Instruments prescribed in Article 3(1)(i) or (ii) of the Act, those in which monetary information pertaining to said Prepaid Payment Instrument is recorded in the center server managed by the Issuer of said Prepaid Payment Instrument and value information is not recorded in IDs issued to users or in documents, cards, etc.

that are issued together with such IDs.

(4) "Within a certain work area" prescribed in Article 4(4)(iv) of the Order shall mean the following.
  (i) a union of workers based on a sense of cooperation in the workplace, whose work area is in the same workplace;
  (ii) a combination of different workplaces for the same type of job and the same type of organization; or
  (iii) a combination of workplaces for the same type of work but not for the same type of organization.

(5) The "Welfare facility" prescribed in Article 4(4)(iv) of the Order means a facility for employees, which is recognized as a welfare facility under normal social conventions, specifically, a shop, canteen, clinic, barber shop, gymnasium, recreation facility, etc.

(6) Prepaid Payment Instruments prescribed in Article 4(5)(i) of the Order shall mean shopping coupons, etc. issued by "Tomonokai" of department stores.

(7) Prepaid Payment Instruments prescribed in Article 4(5)(ii) of the Order shall not include certificates that are issued outside the travel agency business and for which the holder thereof is supposed to conduct the transactions pertaining to the travel agency business only at the time of using them (so-called "travel gift certificate").

I-2 Method of Calculating Unused Base Date Balance

When a notification, etc., pursuant to Article 14(2), Article 15, or Article 16(1) of the Act, or a report pursuant to Article 23 of the Act is submitted, the amount of Unused Base Date Balance shall be handled as follows.

I-2-1 Method of Calculating Unused Base Date Balance

(1) When calculating the amount of Unused Base Date Balance as of the Base Date (which means the Base Date defined in Article 3(2) of the Act; the same applies hereinafter) pursuant to Article 4 of the Cabinet Office Order on Prepaid Payment Instruments (Cabinet Office Order No. 3 of 2010; hereinafter referred to as "Cabinet Office Order"), the amount may be calculated by adding the amount obtained by deducting the amount collected during the Record Period (meaning the amount calculated on the relevant Base Date pursuant to Article 48(2) of the Cabinet Office Order as the amount to be collected of the Prepaid Payment Instruments during the Record Period including the relevant Base Date) from the amount issued during the Record Period (meaning the amount calculated on the relevant Base Date pursuant to Article 48(1) of the Cabinet Office Order as the amount issued of Prepaid Payment Instruments issued during the Record Period including the relevant Base Date) to the Unused Base Date Balance as of the Base Date immediately preceding the relevant Base Date (for the Prepaid Payment Instruments prescribed in Article 3(1)(ii) of the Act, the monetary amount converted from the quantity of goods or services that served as the basis of the calculation as of the Base date). (Note)

Note: In a case to which Article 29-2(1) of the Act applies, if the Record Period containing the date of submission of the notification set forth in the same paragraph is from the day following the special Base Date to the next ordinary Base date, the "Base Date immediately preceding" shall be the ordinary Base Date immediately preceding the

special Base Date, and the "the Record Period including the relevant Base Date" shall be the Record Period including the next ordinary Base Date, and the Record Period immediately preceding the relevant Record Period.

(2) The term "Unused Base Date Balance" as used in (1) above shall also include the issued amount balance of Prepaid Payment Instruments that were recorded in the financial statements as revenue (so-called "taizo-eki (gain from expired Prepaid Payment Instruments)") according to tax regulations.

(3) If the certificates, etc. or numbers, markings, or other symbols that fall under the category of Prepaid Payment Instruments are issued partially for free of charge, the Issuer thereof may determine not to record the amount issued for free of charge in the amount issued, the amount collected, and the unused balance of such Prepaid Payment Instruments only when all of the following requirements are satisfied.

(i) when it is possible to clearly distinguish between those issued for value and those issued free of charge by the content of provision of information or the design of the Prepaid Payment Instruments; and

(ii) when the amount issued, the amount collected, and the unused balance are managed in the books and documents in a manner such that they are clearly distinguished between those issued for value and those issued free of charge.

I-2-2 Special Cases of Method of Calculating Unused Base Date Balance

In the case where a credit lender is an Issuer of Prepaid Payment Instruments, if the amount of receivable for Prepaid Payment Instruments purchased with credit is known, the amount of such receivable portion may be deducted from the amount of the Unused Base Date Balance.

II. Items to Assess in Supervising Issuers of Prepaid Payment Instruments

II-1 Compliance with Laws and Regulations, etc.

II-1-1 Legal Compliance Framework, etc.

It is important for Issuers of Prepaid Payment Instruments to strictly comply with relevant laws and regulations and endeavor to conduct sound and appropriate business operations while recognizing that Prepaid Payment Instruments are one of the important means of payment because this will increase users' confidence in Prepaid Payment Instruments and enhance their convenience through further distribution and development of Prepaid Payment Instruments.

When establishing a control environment for conducting sound and appropriate business operations in strict compliance with laws and regulations, it is important for the management team of Issuers of Prepaid Payment Instruments to give consideration to the realization of sound and appropriate business operations and appropriately exercise its command and supervision function, recognizing the importance of establishing such a control environment.

In addition, even if an Issuer of Prepaid Payment Instruments fails to respond literally as described in each of the viewpoints in these Guidelines, it shall not be regarded as inappropriate if it is deemed that there are no particular problems from the viewpoint of protecting the interests of users of Prepaid Payment Instruments in light of the scale and characteristics of such Issuer of Prepaid Payment Instruments.

When supervising Issuers of Prepaid Payment Instruments, the following points, for example, shall be taken into consideration.

II-1-1-1 Major Supervisory Viewpoints

(i) Has the Issuer of Prepaid Payment Instruments formulated a basic policy on compliance, a specific implementation plan (Compliance Program), and a code of conduct (Code of Ethics and Compliance Manual), etc., and reviews them periodically or as needed? Also, are these documents (policy, plan, and program, etc.) thoroughly disseminated to officers, and employees and other staff who are engaged in the business of issuing Prepaid Payment Instruments (hereinafter referred to as "officers and employees") in order for them to fully understand, and put into practice in daily business operations?

(ii) Is the management team fully aware that banning and eliminating relations with anti-social forces in a resolute manner is essential for the appropriateness of the businesses of Issuers of Prepaid Payment Instruments? And has the management team decided a basic policy in light of the details of "Guidelines for Enterprises to Prevent Damage Caused by Anti-Social Forces" (Agreement at a Meeting of Cabinet Ministers Responsible for Anti-Crime Measures, issued on June 19, 2007; hereinafter referred to as the "Government Guidelines" in II-1-1) and declared it both internally and externally?

Moreover, does the management team clearly define the prevention of damage from anti-social forces as one of the issues in the firm's compliance and risk management? For example, are frameworks to realize the basic policy based on the Government Guidelines developed? And is the effectiveness of those systems verified on a regular basis?

(iii) Does the Issuer of Prepaid Payment Instruments conduct its business operation appropriately in accordance with laws and regulations? Does the Issuer of Prepaid Payment Instruments verify whether the business of issuing Prepaid Payment Instruments is conducted in compliance with laws and regulations and in an appropriate manner, for example, by conducting monitoring and verification by the Internal Control Department and internal audit by the Internal Audit Department? Also, does it promptly improve the inappropriate handling discovered through the verification, etc.?

Note 1: The term "Internal Control Department" as used in these Guidelines refers to the divisions in charge of management of internal affairs, the legal division, etc. for ensuring business operations in compliance with laws and regulations as well as internal rules, etc. In addition, the term "Internal Audit Department" refers to the divisions in charge of inspection, the divisions in charge of auditing, etc. independent from the sales departments, and does not include inspections, etc. conducted by the departments, etc. that are subject to audit as part of internal control.

Note 2: In cases where it is considered more effective to conduct an external audit by an external auditor or an investigation by a Certified Association for Payment Service Providers (hereinafter referred to as the "external audit, etc.") in light of the scale, etc. of the Issuer of Prepaid Payment Instruments, the external audit, etc. may be used in lieu of the internal audit.

(iv) Does the management team of the Issuer of Prepaid Payment Instruments conduct the business of issuing Prepaid Payment Instruments with an understanding of the legal nature of Prepaid Payment Instruments which oblige the issuer to provide goods and services to the users thereof by itself or through its member shops (hereinafter referred to as "Issuer, etc.")?

For example, does the Issuer recognize that it is important to accurately identify not only the cash flows resulting from the issuance of Prepaid Payment Instruments but also the unused balance thereof? And is the Issuer making efforts to develop a system for implementing this?

(v) Does the management team have a policy for issuing Prepaid Payment Instruments that places too much emphasis on the cash flows resulting from the issuance of said Prepaid Payment Instruments in a manner that the remaining balance of said Prepaid Payment Instruments significantly exceeds the ability of the Issuer, etc. of Prepaid Payment Instruments to provide goods and services?

II-1-1-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning control environment of an Issuer of Prepaid Payment Instruments for compliance with laws and regulations, etc., which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-1-2 Prevention of Damage that May be Inflicted by Anti-Social Forces

Eliminating anti-social forces from society is a task critical to ensuring the order and safety of society, so it is necessary and important for corporations to promote efforts to ban any relations with anti-social forces from the viewpoint of fulfilling their social responsibility. It is required to exclude anti-social forces from financial transactions in order to prevent not only Issuers of Prepaid Payment Instruments themselves and their officers and employees, but also their users and other stakeholders from suffering damage inflicted by anti-social forces.

Needless to say, if Issuers of Prepaid Payment Instruments are to maintain the soundness and appropriateness of their business operations, it is essential that they deal with anti-social forces in accordance with laws and regulations without bowing to pressure from them. Therefore, Issuers of Prepaid Payment Instruments must strive, on a daily basis, to develop a control system for banning any relations with anti-social forces in accordance with the purpose of the “Guidelines for Enterprises to Prevent Damage Caused by Anti-Social Forces” (Agreement at a Meeting of Cabinet Ministers Responsible for Anti-Crime Measures, issued on June 19, 2007).

In particular, anti-social forces in recent times have become increasingly sophisticated in their efforts to obtain funds, disguising their dealings as legitimate economic transactions through the use of affiliated companies in order to develop business relations with ordinary companies. In some cases, the relations thus developed eventually lead to problems. In order to deal with such cases properly,

the management team of Issuers of Prepaid Payment Instruments need to take a resolute stance and implement specific countermeasures.

It should be noted that if an Issuer of Prepaid Payment Instruments delays specific actions to resolve a problem involving anti-social forces on the grounds that unexpected situations, such as threats to the safety of its officers and employees, could otherwise arise, the delay could increase the extent of the damage that may be ultimately inflicted on the Issuer of Prepaid Payment Instruments and its officers and employees, etc.

(Reference) "Guidelines for Enterprises to Prevent Damage Caused by Anti-Social Forces"
(Agreement at a Meeting of Cabinet Ministers Responsible for Anti-Crime Measures on June 19, 19)

(i) Basic principles on prevention of damage that may be inflicted by anti-social forces
- ○ Firm-wide response
- ○ Cooperation with external expert organizations
- ○ Ban on any relations, including transactions, with anti-social forces
- ○ Legal responses, both civil and criminal, in the event of an emergency
- ○ Prohibition of engagement in secret transactions with and provision of funds to anti-social forces

(ii) Identification of anti-social forces

In judging whether specific groups or individuals constitute "anti-social forces," which are defined as groups or individuals that pursue economic profits through the use of violence, threats, and fraud, it is necessary not only to pay attention to whether they fit the definition in terms of their affiliation, such as whether they constitute or belong to "Boryokudan" crime syndicates, "Boryokudan" affiliated companies, "Sokaiya" racketeer groups, groups engaging in criminal activities under the pretext of conducting social campaigns or political activities, and crime groups specialized in intellectual crimes, but also to whether they fit the definition in terms of the nature of their conduct, such as whether they are committing violent acts of demand, or making unreasonable demands that go beyond the limits of legal liability (refer to the "Key Points of Measures against Organized Crime," a directive issued in the name of the Deputy Commissioner-General of the National Police Agency on December 22, 2011).

II-1-2-1 Major Supervisory Viewpoints

When examining the control environment of an Issuer of Prepaid Payment Instruments for banning any relationship with anti-social forces and for dissolving any relations with anti-social forces as soon as possible after the counterparty has been found to be an anti-social force in cases where it has established a relationship with an anti-social force unwittingly, as well as the control environment for dealing with unreasonable demands by anti-social forces appropriately, the supervisory authorities, while also giving consideration to the characteristics of specific transactions, shall pay attention to the following points.

(1) Firm-wide response

In light of the need and importance of an action to ban any relationship with anti-social forces organically, does the Issuer of Prepaid Payment Instruments respond to the matter as an organization through appropriate engagement of the management team rather than leaving it solely to the person or department in charge? Does the Issuer of Prepaid Payment Instruments make efforts as a group to eliminate anti-social forces in order to ban the relationship with

anti-social forces not only in the Issuer of Prepaid Payment Instruments itself but also in the business of issuing Prepaid Payment Instruments? Moreover, is there a policy to exclude anti-social forces when providing payment services with cooperation of other companies outside the group (payment service agencies, etc.)?

(2) Development of a centralized control environment through Anti-Social Forces Response Division

Has the Issuer of Prepaid Payment Instruments established a division in charge of supervising responses to ban any relationship with anti-social forces (hereinafter referred to as "Anti-Social Forces Response Division") so as to develop a centralized control environment for preventing infliction of damage by anti-social forces? Is this division properly functioning?

In particular, does the Issuer of Prepaid Payment Instruments pay sufficient attention to the following points in developing the centralized control environment?

(i) Does the Anti-Social Forces Response Division actively collect and analyze information on anti-social forces? Has it developed a database to manage such information in a centralized manner? And does it have a system to appropriately update it (such as addition, deletion, or change of information in the database)? Further, is the Anti-Social Forces Response Division making efforts to share information within the group in the process of collecting and analyzing such information, while making active use of information provided by external expert organizations such as the police, the Center for Removal of Criminal Organizations, and lawyers? In addition, does the Anti-Social Forces Response Division have a system to take advantage of such information on anti-social forces for screening counterparties of transactions including member shops and evaluating the attributes of shareholders of the Issuer of Prepaid Payment Instruments?

(ii) Does the Issuer of Prepaid Payment Instruments make sure to maintain the effectiveness of measures to ban any relations with anti-social forces by, for example, having the Anti-Social Forces Response Division develop a manual for dealing with anti-social forces, provide on-going training, and foster cooperative relationships with external expert organizations such as the police, the Center for Removal of Criminal Organizations, and lawyers on an ongoing basis? In particular, is the Issuer of Prepaid Payment Instruments prepared to report to the police immediately when it faces the imminent prospect of being threatened or becoming the target of an act of violence, by maintaining close communications with the police on a daily basis so as to develop a systematic reporting system and build a relationship that facilitates cooperation in the event of a problem?

(iii) Does the Issuer of Prepaid Payment Instruments have a structure in which relevant information is swiftly and appropriately conveyed to the Anti-Social Forces Response Division for consultation when transactions with anti-social forces are found or such forces have made unreasonable demands? Further, does the Anti-Social Forces Response Division have a structure to swiftly and appropriately report relevant information to the management team? In addition, does the Anti-Social Forces Response Division have a structure to ensure the safety of individuals encountering anti-social forces in person and to support divisions involved in dealing with them?

(3) Implementation of appropriate prior screening

Does the Issuer of Prepaid Payment Instruments take measures to ban allowing anti-social forces to become a counterparty to a transaction including member shops, by conducting

appropriate advance screening using information, etc. on anti-social forces to prevent transactions with anti-social forces, and making sure to insert provisions regarding the exclusion of organized crime group in all contracts and terms of transactions?

(4) Implementation of appropriate follow-up review
Has the Issuer of Prepaid Payment Instruments established a framework for conducting an appropriate follow-up review on existing contracts for the purpose of making sure that any relationships with anti-social forces are eliminated?

(5) Efforts to terminate transactions with anti-social forces
(i) Does the Issuer of Prepaid Payment Instruments have a system under which the information confirming the existence of a transaction with anti-social forces is swiftly and appropriately reported to the management team via the Anti-Social Forces Response Division, and response to the situation is made under appropriate directions and involvement by the management team?
(ii) Does the Issuer of Prepaid Payment Instruments encourage termination of transactions with anti-social forces in close cooperation with external expert organizations such as the police, the Center for Removal of Criminal Organizations, and lawyers on an ongoing basis?
(iii) Does the Issuer of Prepaid Payment Instruments take care to prevent the provision of benefits to anti-social forces, such as severing the relationship as soon as possible if the counterparty has been found to be anti-social forces after initiation of a transaction through a follow-up review, etc.?
(iv) Does the Issuer of Prepaid Payment Instruments have a structure to prevent providing funds or engaging in inappropriate or unusual transactions for whatever reason if the counterparty has been found to be an anti-social force?

(6) Dealing with unreasonable demands by anti-social forces
(i) Does the Issuer of Prepaid Payment Instruments have a system under which the information that anti-social forces have made unreasonable demands is swiftly and appropriately reported to the management team, including directors, etc., via the Anti-Social Forces Response Division, and response to the situation is made under appropriate directions and involvement by the management team?
(ii) Does the Issuer of Prepaid Payment Instruments actively consult external expert organizations such as the police, the Center for Removal of Criminal Organizations, and lawyers on an ongoing basis when anti-social forces make unreasonable demands, and respond to such unreasonable demands based on guidelines set by the Center for Removal of Criminal Organizations and other organizations? In particular, does the Issuer of Prepaid Payment Instruments have a structure to report to the police immediately when there is an imminent prospect of a threat being made or an act of violence being committed?
(iii) Does the Issuer of Prepaid Payment Instruments have a policy to take every possible civil legal action against unreasonable demands by anti-social forces and to avoid hesitating to seek the initiation of a criminal legal action, by proactively reporting damage to the relevant authorities?
(iv) Does the Issuer of Prepaid Payment Instruments ensure that the division in charge of handling problematic conduct promptly conducts a fact-finding investigation upon request from the Anti-Social Forces Response Division, in cases where unreasonable demands from

anti-social forces are based on problematic conduct related to business activity or involving any of its officers or employees?

(7) Management of shareholder information

Does the Issuer of Prepaid Payment Instruments manage shareholder information properly, through means such as regularly checking the transaction status of its own shares and examining information regarding the attributes of its shareholders?

II-1-2-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning the control environments to ban relationship with anti-social forces of an Issuer of Prepaid Payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider necessary measures of strict dispositions based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-1-3 Actions to Misconduct

In case of occurrence of “an act in violation of laws and regulations with regard to the business of issuing Prepaid Payment Instruments or an act that hinders the sound and appropriate operation of the business of issuing Prepaid Payment Instruments by itself or any of its officers or employees” as set forth in Article 53-2 of the Cabinet Office Order (hereinafter referred to as “misconduct”), the following supervisory actions shall be taken.

Misconduct shall mean and include the following acts in addition to acts in violation of laws and regulations in relation to the business of issuing Prepaid Payment Instruments.

- Fraud, embezzlement, breach of trust, etc. in relation to the business of issuing Prepaid Payment Instruments; which is likely to harm the interests of users thereof;
- An of being subject to a complaint or accusation by a user, or arrest with regard to the business of issuing Prepaid Payment Instruments; and
- An act equivalent to those listed above that hinders or is likely to hinder the sound and appropriate operation of the business of issuing Prepaid Payment Instruments.

II-1-3-1 Major Supervisory Viewpoints

(i) In cases where any misconduct is found at an Issuer of Prepaid Payment Instruments and the supervisory authorities receive an initial notice from said Issuer of Prepaid Payment Instruments, the supervisors shall confirm the following points. The same shall apply to the case where no initial report has been made by an Issuer of Prepaid Payment Instruments but

a written notification has been submitted by that Issuer.

(A) Whether the Issuer of Prepaid Payment Instruments has made a prompt report to the Internal Control Department and a report to the management team in accordance with internal rules, etc.

(B) In cases where the act could constitute a criminal offense, whether the Issuer of Prepaid Payment Instruments has reported it to the police and other relevant organizations.

(C) Whether the Issuer of Prepaid Payment Instruments has investigated and clarified the misconduct at an independent department (Internal Audit Department, etc.)

(ii) The supervisors examine the appropriateness of the business of issuing Prepaid Payment Instruments in relation to the misconduct based on the following viewpoints.

(A) Whether the Issuer of Prepaid Payment Instruments appropriately acted immediately after the misconduct came to light.

(B) Whether the management team has been involved in the misconduct and whether there has been firm-wide involvement.

(C) What impacts the misconduct is expected to have on users of Prepaid Payment Instruments.

(D) Whether the internal check-and-balance function is properly working.

(E) Whether the Issuer of Prepaid Payment Instruments has formulated improvement measures to prevent recurrence and sufficient self-cleaning functions, and whether it has clearly pursued the responsibilities of the parties concerned.

(F) Whether the Issuer of Prepaid Payment Instruments has made appropriate explanations to users thereof and responded to inquiries.

II-1-3-2 Supervisory Methods and Measures

When receiving a notification of misconduct from an Issuer of Prepaid Payment Instruments, the supervisory authorities shall monitor the status of voluntary business improvement made by the Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the facts (the business office where the misconduct occurred, the name, title, and job history of the person who committed such misconduct, a summary of the misconduct, the date when the misconduct was detected, the period of the misconduct, why the misconduct was detected), analysis of the cause of the misconduct, and improvement and response measures against the misconduct, and collecting a report based on Article 24 of the Act when necessary.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-2 Provision of Information and Consultation Function, etc. for Protection of Users

II-2-1 Obligation to Provide Information

Since issuing Prepaid Payment Instruments means receiving credit from users of Prepaid Payment Instruments, it is very important to clarify the status of such credit from the viewpoint of protecting

the interests of the users thereof.
In addition, as there are various types of Prepaid Payment Instruments, such as certificate type, IC card type, and server-type, it is necessary to appropriately provide information according to each type.

II-2-1-1 Major Supervisory Viewpoints

(i) In the case of Prepaid Payment Instruments for which information is provided by the method prescribed in Article 21(1) of the Cabinet Office Order, in accordance with said paragraph, is the information specified in each item of Article 13(1) of the Act entered without omission? (Notes 1 and 2)

(ii) In the case of Prepaid Payment Instruments for which information is provided by the methods prescribed in each item of Article 21(2) of the Cabinet Office Order, does the Issuer of Prepaid Payment Instruments follow a procedure to confirm the information on the matters prescribed in each item of Article 13(1) of the Act without fail when a user purchases Prepaid Payment Instruments from the Issuer (excluding cases where said Prepaid Payment Instruments are Addition-Type Prepaid Payment Instruments and said addition is made)? Also, is it possible for a user to check such information even after purchasing the Prepaid Payment Instruments? (Note 1)

(iii) Does the Issuer of Prepaid Payment Instruments provide users of Prepaid Payment Instruments with the matters prescribed in each item of Article 23-2(1) of the Cabinet Office Order without omission by a reasonable method based on actual practice to the extent that it will not prevent accurate understanding by users?

(iv) Is the policy relating to compensation for losses of users and other response prescribed in Article 23-2(1)(iii) of the Cabinet Office Order based on II-2-9 hereof?

Note 1: In cases where the Issuer of Prepaid Payment Instruments is a member of a Certified Association for Payment Service Providers, it should be noted that a part of the items subject to the obligation to provide information is permitted to be posted on the website of such Certified Association for Payment Service Providers pursuant to Article 13(2) of the Act and Article 23-2(3) of the Cabinet Office Order.

Note 2: The term “documents or other materials that are an integral part of the Prepaid Payment Instruments” prescribed in Article 21(1) of the Cabinet Office Order means those that are required to be presented or delivered by a user when using the Prepaid Payment Instruments, and it should be noted that the term does not include those merely indicating the number, marking, or other symbol of Prepaid Payment Instruments that a user does not have to present or deliver when using the Prepaid Payment Instruments.

II-2-1-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning the obligation of an Issuer of Prepaid Payment Instruments to provide information, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.
In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the

viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-2-2 Books and Documents

The obligation to prepare and preserve books and document on the business of issuing Prepaid Payment Instruments is stipulated by law in order to contribute to the protection of the interests of users of Prepaid Payment Instruments by accurately reflecting the amount of issuance of Prepaid Payment Instruments and the unused balance thereof and requiring the deposit of a security deposit for issuance, etc. based on the entry in said books. When examining the preparation and preservation of the books and documents, the following points shall be taken into consideration in light of the abovementioned intent.

II-2-2-1 Major Supervisory Viewpoints

(i) Has the Issuer of Prepaid Payment Instruments developed systems to appropriately prepare and preserve books and documents on the business of issuing Prepaid Payment Instruments? For example, are the following systems established?

(A) Has the Issuer of Prepaid Payment Instruments established a control environment in which the number of issues, the volume of issues, the number of those in stock, and the volume of those already collected can be periodically ascertained for each type of Prepaid Payment Instrument, and the amount available for payment, etc. thereof? In addition, if it is deemed difficult to ascertain the volume of those already collected by each type of the amount available for payment, etc. of Prepaid Payment Instruments, has the Issuer of Prepaid Payment Instruments established a control environment in which the amount of the volume of those already collected can be ascertained by the type of Prepaid Payment Instrument? (Note)

(B) In cases where the certificates, etc. are issued at multiple locations, does the headquarters of the Issuer of the Prepaid Payment Instrument accurately grasp the number of those issued and the number of those in stock at each issuance location?

(C) In cases where the Issuer of Prepaid Payment Instruments has issued the Prepaid Payment Instruments as prescribed in Article 3(1)(ii) of the Act, has it established a control environment in which the normal offering price per unit of the goods, etc. pertaining to said Prepaid Payment Instruments can be ascertained?

(ii) Does any department, such as the Internal Audit Department, other than the Books-and-Documents-Preparation Division, verify the accuracy of the description of the books and documents?

(iii) In the case where books and documents are prepared electronically, is there a control environment in which books and documents can be restored when data are damaged, for example, via periodic back-up of books and documents, etc.?

Note: It should be noted that even with regard to Prepaid Payment Instruments with an expiration date, if the Issuer of Prepaid Payment Instruments actually permits users to use them after the expiration date thereof, the Issuer of Prepaid Payment Instruments

is not allowed to deduct those expired from the unused balance of issued Prepaid Payment Instruments.

II-2-2-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning the preparation and preservation of the books and documents of an Issuer of Prepaid Payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-2-3 Control Environments for Management of User Information

Information regarding individual users of Prepaid Payment Instruments needs to be handled in an appropriate manner in accordance with the provisions of Articles 44 and 45 of the Cabinet Office Order as well as the Act on the Protection of Personal Information (Act No. 57 of 2003, hereinafter referred to as the "Personal Information Protection Act") as well as the Guidelines on the Act on the Protection of Personal Information; (General rules), (Provision to foreign third parties), (Obligation to confirm and record at the time of provision to third parties), (Anonymized information) (hereinafter collectively referred to as the "Personal Information Protection Guidelines"), the Guidelines on the Protection of Personal Information in the Financial Sector (hereinafter referred to as the "Financial Sector Personal Information Protection Guidelines"), and the Guidelines for Practical Affairs regarding Safety Control Measures specified in the Guidelines on the Protection of Personal Information in the Financial Sector (hereinafter referred to as the "Practical Guidelines").

In addition, personal information including credit card information (number and expiration date, etc.)(hereinafter referred to as "credit card information, etc.") needs to be strictly managed because secondary damage such as spoofed purchase via unauthorized use of such information may occur if it is leaked.

In light of the above, when supervising Issuers of Prepaid Payment Instruments, the following points, for example, shall be taken into consideration.

II-2-3-1 Major Supervisory Viewpoints

(1) Control environments for management of user information

(i) Does the management team of the Issuer of Prepaid Payment Instruments recognize the necessity and importance of ensuring the appropriateness of managing information of users? Has the Issuer of Prepaid Payment Instruments developed an internal control environment, such as establishing an organizational structure (including establishing appropriate checks

between divisions) and formulating internal rules to ensure the appropriate management of such information?

(ii) Has the Issuer of Prepaid Payment Instruments formulated a specific standard for the handling of user information and communicated it to all officers and employees through the provision of training and other means? In particular, with regard to the transmission of such information to third parties, has the Issuer of Prepaid Payment Instruments established the handling standard after sufficient consideration to ensure that procedures are carried out in accordance with the provisions of the aforementioned laws and regulations, the Personal Information Protection Guidelines, the Financial Sector Personal Information Protection Guidelines, and the Practical Guidelines?

(iii) Has the Issuer of Prepaid Payment Instruments established frameworks necessary for examining the management status of user information in a timely and appropriate manner? Such frameworks include management of access to user information (such as preventing access rights assigned to certain people from being used by others), measures to prevent the misappropriation of user information by insiders, and a robust information management system that prevents unauthorized access from the outside.

Also, has the Issuer of Prepaid Payment Instruments taken appropriate measures for preventing wrongful acts utilizing user information, such as the dispersal of authority concentrated upon specific personnel and the enhancement of controls and checks over personnel who have broad powers?

(iv) Has the Issuer of Prepaid Payment Instruments established frameworks for appropriately reporting to responsible divisions when user information has been leaked, and notifying relevant users, reporting to the relevant authorities, and disclosing to public in a prompt and appropriate manner to prevent secondary damage?

Also, does the Issuer of Prepaid Payment Instruments analyze the causes of information leaks and implement measures designed to prevent recurrence? Furthermore, in light of incidents of information being leaked at other companies, does the Issuer of Prepaid Payment Instruments examine measures needed to prevent a similar incident from occurring in its organization?

(v) Does the Issuer of Prepaid Payment Instruments conduct audits covering the broad range of business operations handling user information by its independent Internal Audit Department on a periodic or as-needed basis?

Also, has the Issuer of Prepaid Payment Instruments implemented appropriate measures, such as training programs, in order to increase the specialization of the staff engaged in audits pertaining to the management of user information?

(vi) With regard to an Issuer of Prepaid Payment Instruments who is a member of a Certified Association for Payment Service Providers, does the Issuer of Prepaid Payment Instruments regularly have its officers and employees participate in training sponsored by the Certified Association for Payment Service Providers or equivalent training in order to ensure the appropriate handling of information?

Also, with regard to an Issuer of Prepaid Payment Instruments who is not a member of a Certified Association for Payment Service Providers, does the Issuer of Prepaid Payment Instruments regularly have its officers and employees participate in training with equivalent content to that mentioned above in order to ensure the appropriate handling of information?

(2) Management of personal information

(i) With regard to information concerning individual users, has the Issuer of Prepaid Payment Instruments implemented the following necessary and appropriate measures for its safe management and supervision of persons in charge in order to prevent such information from being leaked, lost, or damaged, in accordance with Article 44 of the Cabinet Office Order?

(Necessary and appropriate measures concerning safety management)

(A) Measures based on Article 8 of the Financial Sector Personal Information Protection Guidelines

(B) Measures based on I, and Appendix 2 of the Practical Guidelines

(Necessary and appropriate measures concerning supervision of persons in charge)

(C) Measures based on Article 9 of the Financial Sector Personal Information Protection Guidelines

(D) Measures based on II of the Practice Guidelines

(ii) Has the Issuer of Prepaid Payment Instruments implemented measures to ensure that information regarding the race, religious beliefs, family origin, registered domicile, healthcare, and criminal records of individual users, as well as other specified non-disclosure information (Note), are not used except for the cases specified in each item under Article 5(1) of the Financial Sector Personal Information Protection Guidelines?

Note: Other specified non-disclosure information includes the following;

(A) Information regarding labor union membership

(B) Information regarding ethnicity

(C) Information regarding sexual orientation

(D) Information regarding matters set forth in Article 2(iv) of the Cabinet Order to Enforce the Act on the Protection of Personal Information

(E) Information regarding matters set forth in Article 2(v) of the Cabinet Order to Enforce the Act on the Protection of Personal Information

(F) Information regarding facts that he/she has suffered damage by crime

(G) Information regarding social status

(iii) For credit card information, etc., has the Issuer of Prepaid Payment Instruments implemented the following measures?

(A) Has the Issuer of Prepaid Payment Instruments set an appropriate period of time for keeping credit card information, etc., which takes into account the purpose of use and other circumstances? Does it limit the locations where such information is kept, and dispose of the information in a prompt and appropriate manner after the retention period has lapsed?

(B) Has the Issuer of Prepaid Payment Instruments implemented appropriate measures when displaying credit card information, etc. on computer monitors, such as not displaying whole credit card numbers, unless needed for business operations?

(C) Does the independent Internal Audit Department of the Issuer of Prepaid Payment Instruments conduct internal audit on a periodic or as-needed basis on whether the rules and systems for protecting credit card information, etc. are functioning effectively?

(iv) Has the Issuer of Prepaid Payment Instruments taken measures to comply with Article 12 of the Financial Sector Personal Information Protection Guidelines and other applicable provisions with regard to the provision of personal data to third parties? In particular, does the Issuer of Prepaid Payment Instruments obtain consents from individual users while

paying attention to the following points according to the nature and methods of the business?

(A) When obtaining a consent from an individual user for the provision of his/her information to a third party in a non-face-to-face manner such as via PC or smartphone, etc., has the Issuer of Prepaid Payment Instruments designed the relevant webpage so that individual customers can easily understand the content and purpose of use of information provided to such third party by making it more customer-friendly in terms of the text of consent, letter size, screen specifications, manner of giving consent, etc. in accordance with Article 3 of the Financial Sector Personal Information Protection Guidelines?

(B) Even in the case where the Issuer of Prepaid Payment Instruments has obtained a consent for the provision of personal information to a third party from an individual user in the past, if the third party to which the information is provided or the content of information to be provided is different from the past case or if the scope of provision of such information exceeds the necessary extent to achieve a utilization purpose specified before, does the Issuer of Prepaid Payment Instruments obtain a consent from such individual user again?

(C) In cases where personal information of individual users is provided to multiple third party contractors or where the purpose of use of personal information varies at each third party contractor, does the Issuer of Prepaid Payment Instruments consider the scope of the third parties for which a consent of the user must be obtained, and how and when to obtain such consent in a proper manner so that the individual users are able to understand the fact that their information will be provided to multiple third parties, as well as the purpose of use at each third party contractor?

(D) In obtaining a consent for the provision of personal information to third parties, is the Issuer of Prepaid Payment Instruments mindful not to cause any risk of abuse of superior position or conflict on interests between it and the individual user? For example, is an individual user forced to give a consent beyond the reasonable scope of provision in terms of the third parties to which the personal information is provided, the purpose of use, or the content of information to be provided?

II-2-3-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning control environment of an Issuer of Prepaid Payment Instruments for management of user information, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into

consideration when conducting administrative dispositions).

Note: With regard to the handling of personal information, note that there are some cases in which necessary measures should be taken according to the delegation of authority to the competent minister for the relevant business under the Act on the Protection of Personal Information as needed.

II-2-4 Control Environment for Complaint Processing

When supervising Issuers of Prepaid Payment Instruments in terms of control environment for complaint processing, the following points, for example, shall be taken into consideration.

II-2-4-1 Major Supervisory Viewpoints

(i) Efforts made by Issuer of Prepaid Payment Instruments to respond to complaints, etc.

Has the management team of the Issuer of Prepaid Payment Instruments taken appropriate measures, recognizing that it may suffer disadvantages such as loss of confidence due to complaints, etc. from users?

(ii) Establishment of complaint processing system

Has the Issuer of Prepaid Payment Instruments established a division in charge of complaints, etc. and procedures for processing them so that complaints, etc. can be processed and dealt with promptly and appropriately? Does the Issuer of Prepaid Payment Instruments have a system for sharing information among relevant parties as necessary according to the case, such as reporting to the Internal Audit Department and the management team if a complaint, etc. could have a material impact on the management thereof?

(iii) With regard to complaints, etc. pertaining to the use of Prepaid Payment Instruments at member shops, has the Issuer of Prepaid Payment Instruments developed an appropriate complaint consultation system, such as a system to accept direct communication from users, etc. to the Issuer of Prepaid Payment Instruments?

(iv) Explanation to users

Has the Issuer of Prepaid Payment Instruments developed a control environment for sincerely responding to complaints, etc., such as providing sufficient explanations to users, obtaining their understanding and consent, and resolving them? Also, has the Issuer of Prepaid Payment Instruments appropriately followed up the status of responding to complaints, etc.?

(v) Feedback

Does the Issuer of Prepaid Payment Instruments properly and accurately record and keep the contents of complaints, etc. and results of measures taken therefor? Also, has the Issuer of Prepaid Payment Instruments developed a control environment wherein it analyzes the contents of complaints, etc. and the result of handling them, and applies this on an ongoing basis to the improvement of control environments for dealing with users and conducting administrative processes and to the formulation of measures for preventing any occurrence or recurrence of complaints?

(vi) With regard to an Issuer of Prepaid Payment Instruments who is a member of a Certified Association for Payment Service Providers, does the Issuer of Prepaid Payment Instruments endeavors to resolve disputes promptly by actively cooperating with the association in resolving the dispute?

II-2-4-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning control environment of an Issuer of Prepaid Payment Instruments for complaint processing, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-2-5 Response to Fictitious Billing and Other Fraud Damage Caused by Abuse of Server-type Prepaid Payment Instruments

Some Prepaid Payment Instruments can be easily purchased and used by anyone at a store anonymously, and can be transferred to others. In particular, some Server-type Prepaid Payment Instruments have the characteristic of being able to be used by inputting an ID on the Internet without presenting or issuing the certificates, etc., and have become widespread as a means of settlement along with the expansion of Internet transactions.

In this way, Prepaid Payment Instruments have spread as a means of settlement that is highly convenient for users. On the other hand, users face troubles exploiting this characteristic, such as being cheated to purchase a Server-type Prepaid Payment Instruments via fictitious billing and having their IDs stolen.

In light of these circumstances, Issuers of Server-type Prepaid Payment Instruments for which fictitious billing and other fraud damage are recognized are required to make efforts to prevent fraud and recover from damage through monitoring and analysis of the status of occurrence of fraud.

When supervising Issuers of Prepaid Payment Instruments in terms of response to fictitious billing and other fraud damage, the following points, for example, shall be taken into consideration.

Even if an Issuer of Server-type Prepaid Payment Instruments fails to respond literally as described hereunder, it is not inappropriate if it is deemed that there are no particular problems from the viewpoint of preventing damage, etc. in light of the scale and characteristics of such Issuer of Server-type Prepaid Payment Instruments.

II-2-5-1 Major Supervisory Viewpoints

(i) Has the Issuer of Prepaid Payment Instruments developed a system for promptly receiving information on fraud damages such as claims from victims, etc. (including the provision of information from investigative authorities, consumer affairs centers, etc.; the same applies hereinafter)? And has it developed a control environment for identifying Prepaid Payment Instruments that were stolen, and promptly and appropriately taking measures for suspension of use by utilizing such information, etc.?

(ii) In the case where there is an unused balance of the Prepaid Payment Instruments that are

suspended for use based on a claim from a victim, etc. has the Issuer of Prepaid Payment Instruments developed a control environment for smooth and prompt handling of such unused balance by, for example, establishing refund procedures, etc. (Note) in its internal rules in order to promptly recover the property damage of the victim?

Note: It should be noted that the refund procedures, etc. in the case of the suspension of use based on a claim from a victim of fraud, etc. are not considered to be the refund based on Article 20(5) of the Act. Provided, however, that this shall not preclude such refund from being processed as the refund under Article 20(5) of the Act and each of the items of Article 42 of the Cabinet Office Order from the viewpoint of prompt damage recovery.

(iii) Has the Issuer of Prepaid Payment Instruments developed a control environment in which it promptly and appropriately takes the following measures, for example, in response to ways of fraud involving fictitious billings, from the viewpoint of preventing damage, etc. through monitoring and analysis of the occurrence of damage based on claims from victims, etc.? (See II-2-4 for matters to be noted regarding the environment for complaint processing.)

(A) Indication of warning on the website, etc. of the Issuer of Prepaid Payment Instruments

(B) Indication of warning on a sales terminal at the time of sale and/or a prepaid card, etc. displayed in a shop

(C) Review of sales methods abused for fictitious billing or other fraud (for example, lowering the maximum selling amount for a specific sales channel or type of sales certificate that is being abused, and suspending the handling of such certificates).

II-2-5-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning the response to fictitious billing and other fraud damage of an Issuer of Server-type Prepaid payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Server-type Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Server-type Prepaid Payment Instruments is found to have serious problems from the viewpoint of preventing fictitious billing and other fraud damage and recovering from damage, the supervisory authorities shall issue to the Issuer of Server-type Prepaid Payment Instruments an order to improve business operations based on Article 25 of the Act. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-2-6 Measures to Prevent Inappropriate Use

Along with the development of information and communications technology, among the mechanisms provided by Issuers of Prepaid Payment Instruments, such Prepaid Payment Instruments have emerged that allow holders thereof to transfer their means of payment between individuals by transferring their unused balance.

Such Prepaid Payment Instruments have the advantage in that it is easy to trace the transfer history, because unused balance is transferred repeatedly in the mechanism provided by the Issuer. But, it is considered necessary that the transfer of Prepaid Payment Instruments in the mechanism provided

by the issuer should not be used for inappropriate transactions that would harm public order and morals, for example.

Based on this, an Issuer of Prepaid Payment Instruments who issues Prepaid Payment Instruments prescribed in Article 23(3)(i) of the Cabinet Office Order is required to take necessary measures to prevent the inappropriate use of those Prepaid Payment Instruments (hereinafter referred to as "measures to prevent inappropriate use").

When supervising such Issuer of Prepaid Payment Instruments in terms of the measures to prevent inappropriate use, the following points, for example, shall be taken into consideration.

Even if the Issuer of Prepaid Payment Instruments fails to respond literally as described hereunder, it is not inappropriate if it is deemed that there are no particular problems from the viewpoint of preventing inappropriate use in light of the scale and characteristics of such Issuer of Prepaid Payment Instruments.

II-2-6-1 Major Supervisory Viewpoints

(i) Has the upper limit of transferable unused balance of Prepaid Payment Instruments been set to an reasonable amount according to actual demand, in order that it will not be used for inappropriate transactions?

(ii) Has the Issuer of Prepaid Payment Instruments developed a system for detecting suspicious transactions, such as identifying those who have repeatedly received transfers of a certain amount or more?

(iii) Has the Issuer of Prepaid Payment Instruments taken measures such as temporarily suspending the use of transactions with persons who are engaged in suspicious transactions? Also, does the Issuer of Prepaid Payment Instruments check parties involved in such suspicious transactions and the content thereof as needed?

II-2-6-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning the measures to prevent inappropriate use of an Issuer of Prepaid Payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-2-7 Responses to Persons with Disabilities

The Act for Eliminating Discrimination against Persons with Disabilities (Act No. 65 of 2013; hereinafter referred to as the "Disability Discrimination Act") prohibits a company from engaging in unfair discriminatory treatment for persons with disabilities and requires it to make efforts to

improve reasonable accommodation to implement elimination of social barriers.
In addition, the "Guidelines concerning Promotion of Elimination of Discrimination on the Basis of Disability in Business Fields under the FSA's Jurisdiction" (Public Notice No. 3 of 2016; hereinafter referred to as the "Guidelines for Eliminating Discrimination against Persons with Disabilities") has specified how Issuers of Prepaid Payment Instruments should respond to those with disabilities.
When supervising the response to persons with disabilities, the following points shall be taken into consideration in light of the abovementioned intent.

II-2-7-1 Major Supervisory Viewpoints

Has the Issuer of Prepaid Payment Instruments developed an internal control environment for responding to persons with disabilities, such as by taking appropriate actions in accordance with the Disability Discrimination Act and the Guidelines for Eliminating Discrimination against Persons with Disabilities including in terms of user protection and user convenience, and by grasping and verifying the response status and reviewing response methods?

II-2-7-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning the response to persons with disabilities by an Issuer of Prepaid Payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the development of the relevant internal control environment by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. based on the viewpoints mentioned above. Also, when any doubt arises regarding the development of the internal control environments by the Issuer of Prepaid Payment Instruments, the supervisors shall inspect it, as needed, by requiring the Issuer of Prepaid Payment Instruments to submit a report (including those under Article 24 of the Act). If any problem is found in such development, the supervisors shall encourage the Issuer of Prepaid Payment Instruments to improve.

II-2-8 Linkage with Services Provided by Other Service Providers such as Account Transfer Service

Some Prepaid Payment Instruments are offering services collaborated with services provided by other business operators such as account transfer services provided by banks, etc. (hereinafter referred to as "collaborative service").
While such collaborative service may become highly convenient for users of Prepaid Payment Instruments, there is a possibility of introducing risks different from those inherent in the services provided by an Issuer of Prepaid Payment Instruments alone, for example, a risk that a malicious third party impersonates a depositor of a savings account linked to the Prepaid Payment Instruments (hereinafter referred to as the "linked account") and makes improper transaction through the Prepaid Payment Instruments. In addition, with the progress of innovation of technologies, collaboration and linkage between business operators will increase in the future, and the risk associated with these kind of collaboration may also increase.
Based on the above, from the viewpoint of ensuring sound and appropriate management of the business of issuing Prepaid Payment Instruments including the protection of the interests of users of Prepaid Payment Instruments and users of services provided by business partners (hereinafter referred to as "users, etc." in II-2-8 and II-2-9), it is important for an Issuer of Prepaid Payment Instruments who provides collaborative services to establish a control environment suited to the risks in cooperation with the business partners. When supervising an Issuer of Prepaid Payment

Instruments who provides collaborative services, the supervisors shall pay attention to the following points, for example.

In addition, the following viewpoints are given, mainly assuming the cases of linking with the account transfer service. Similarly, when providing other collaborative services that may cause economic loss to users, etc. due to vulnerability in security, etc., it is important for Issuers of Prepaid Payment Instruments to take necessary measures according to the risk, taking the following points into consideration.

II-2-8-1 Major Supervisory Viewpoints

(1) Development of internal control environment

(i) Does the management team have the Internal Control Department identify inherent risks, including problems pertaining to the protection of the interests of users, etc., with regard to the entire collaborative services at the time of introduction of the services or at the time of any change in the contents and methods thereof, and develop a system to reduce risks in a timely manner based on these?

(ii) Does the Internal Control Department collect and analyze information on the occurrence of relevant crimes and methods thereof based on the types of crimes that are expected to occur in collaborative services? And does it improve the system for the operation of collaborative services (including fraud prevention measures), taking into account possible future crime methods? Also, does it report the content thereof to the management team on a regular and timely basis?

(iii) Does the Internal Audit Department audit the control environment (including fraud prevention measures) for the operation of collaborative services on a regular and timely basis? Also, does it report the audit result to the management team?

(iv) Does the management team create an environment in which the so-called PDCA cycle, which consists of risk analysis, the formulation and implementation of risk mitigation measures, and the evaluation and review thereof, functions as described above?

(2) Security

(i) From the viewpoint of preventing improper transactions, does the Issuer of Prepaid Payment Instruments assess possible risk of the entire collaborative service in cooperation with its business partners at the time of introduction of the services or at the time of any change in the contents and methods thereof? Also, does it cooperate with the business partners in assessing the risk?

(ii) Has the Issuer of Prepaid Payment Instruments clarified the division of roles and responsibilities with the business partners?

(iii) Based on the risk assessment, does the Issuer of Prepaid Payment Instruments crosscheck information on users in cooperation with the business partners, and take appropriate and effective measures commensurate with risks to prevent fraud?

For example, in the case of linking with the account transfer service, does the Issuer of Prepaid Payment Instruments take appropriate and effective measures to prevent unauthorized use, such as notifying depositors at the linked bank accounts via their telephone numbers and addresses registered therewith of information necessary for authentication by the Issuer of Prepaid Payment Instruments (including SMS (short message service) to telephone numbers), and setting the charge limit at a level that is deemed to enable to prevent improper transactions?

Note:In collating information with business partners, it is desirable to include addresses and telephone numbers in addition to the names and dates of birth of users, except when using official personal authentication.

In addition, has the Issuer of Prepaid Payment Instruments confirmed that partner banks, etc. that offer the account transfer service have introduced multi-factor authentication and other authentication methods that combine effective elements, such as, for example, the use of variable passwords using hardware tokens and software tokens, and the use of electronic certificates such as public personal authentication, in addition to the use of fixed ID and passwords for personal authentication?

Note:It should be noted that fraud prevention measures taken by an Issuer of Prepaid Payment Instruments do not overlap with those taken by the partner banks, etc. In addition, it should be kept in mind that the partner banks, etc. must adopt a robust authentication method for registering and changing information used for authentication, such as telephone numbers.

(iv) Does the Issuer of Prepaid Payment Instruments regularly and in a timely manner check and re-evaluate risks in light of changes in the environment, including the sophistication of crime methods, and the occurrence of incidents at the Issuer itself or other business operators, and improve measures to prevent fraud, including the introduction of public personal authentication?

(v) If, as a result of risk assessment, it is found that there is a problem from the viewpoint of ensuring the sound and appropriate operation of the business of issuing Prepaid Payment Instruments, including the protection of the interests of users, etc., does the Issuer of Prepaid Payment Instruments temporarily suspend all or part of its services, including collaborative services, or take other appropriate measures until the problem is resolved?

(3) Notification to users, etc.

When engaging in the linked account transfer service, etc., with business partners, does the Issuer of Prepaid Payment Instruments take measures to enable users, etc. to confirm the fact that such service is a collaborative service and the content of such service in a timely manner by cooperating with the partner to notify users, etc. at their contact information such as the telephone number and e-mail address registered with the partner in advance, so that users, etc. can be aware of fraud or other damage, if any, at an early stage?

Note: When the Issuer of Prepaid Payment Instruments implements the above measures by notifying users, etc. via their contact information registered with the business partner, it should be kept in mind that the Issuer of Prepaid Payment Instrument needs to confirm that the partner has introduced a robust authentication method for registering and changing contacts such as phone numbers and e-mail addresses.

(4) Detection of improper transactions (Monitoring)

With regard to the collaborative services, from the viewpoint of preventing improper transactions, has the Issuer of Prepaid Payment Instruments developed a control environment for appropriately implementing the following matters, for example, in cooperation with business partners?

- To promptly detect transactions suspected of being fraudulent by setting appropriate scenario or thresholds based on changes in the environment, including the sophistication of criminal

methods, and the occurrence of incidents in it or other business entities
- To share information on suspicious transactions detected based on the above with business partners in a timely manner, to take necessary measures including suspension of the services, and to investigate such suspicious transactions
- To promptly notify persons who may be a victim of fraud of the incident
- To suspend the use of IDs that have been confirmed to be used for improper transactions

(5) Response to inquiries from users

(i) Has the Issuer of Prepaid Payment Instruments developed a control environment for accumulating and analyzing cases of inquiries and consultations from users, etc. concerning collaborative services (hereinafter referred to as "inquiries, etc.") and utilizing them for early detection of risks, and for improvement of fraud prevention measures and responses to consultations from users, etc.?

(ii) Has the Issuer of Prepaid Payment Instruments developed a control environment for honestly and sincerely responding to users, including inquiries, etc. on business partners? Also, has it clarified how to cooperate and share the responsibilities with business partners in specific manners?

(iii) Does the Issuer of Prepaid Payment Instruments crosscheck with a business partner whether each of them has taken any inappropriate actions in responding inquiries, etc. from users, etc., such as inducing users, etc. who made an inquiry to either party to contact the other party? And if any inappropriate responses are found, does the Issuer of Prepaid Payment Instruments, together with the partner, properly investigate the cause thereof, take corrective measures and measures to prevent recurrence, etc.?

II-2-8-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning the provision of collaborative services of an Issuer of Prepaid Payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments, including the viewpoint of protecting the interests of the users, etc., the supervisory authorities shall issue to the Issuer of Prepaid Payment Instruments an order to improve business operations based on Article 25 of the Act. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-2-9 Compensation for Damage due to Improper Transactions

Users, etc. may be damaged by improper transactions using Prepaid Payment Instruments.

When such damage occurs, it is important for an Issuer of Prepaid Payment Instruments to take appropriate and prompt measures for the victim (including measures in cooperation with business partners when providing collaborative services) from the viewpoint of ensuring sound and

appropriate management of the business of issuing Prepaid Payment Instruments that includes protection of the interests of users, etc.

When supervising Issuers of Prepaid Payment Instruments in terms of response to improper transactions, the following points, for example, shall be taken into consideration.

II-2-9-1 Major Supervisory Viewpoints

(i) Based on Article 23-2(1)(iii) and Article 23-3(ii) of the Cabinet Office Order, has the Issuer of Prepaid Payment Instruments formulated a policy concerning compensation for damage arising from improper transactions made in connection with the business of issuing Prepaid Payment Instruments and other measures (hereinafter referred to as "Compensation Policy")? And has it provided users of Prepaid Payment Instruments with necessary information and made it available also to persons other than the users of Prepaid Payment Instruments who are likely to incur losses in the event of the occurrence of improper transactions?

Note 1: The "damage arising from improper transactions made in connection with the business of issuing Prepaid Payment Instruments" includes not only any loss and damage incurred by users of Prepaid Payment Instruments arising from instructions given by unauthorized persons against the will of said users, but also any loss and damage incurred by users of a collaborative service provided by the business partner in connection with the provision of the collaborative service, such as loss or damage of an depositor of an account whose account is used for improper account transfer by users of Prepaid Payment Instruments who pretend to be such depositors, against the will of said depositors.

Note 2: The "cases where it is deemed necessary in light of the content and method of the business of issuing Prepaid Payment Instruments" prescribed in Article 23-3(ii) of the Cabinet Office Order means cases where, in light of the content and method of the business of issuing Prepaid Payment Instruments, damage is likely to be incurred by persons other than users of Prepaid Payment Instruments, such as cases of issuance of Prepaid Payment Instruments linked with an account transfer service provided by banks, etc.

(ii) Does the Compensation Policy include at least the following items?

(A) Depending on the contents of business of issuing Prepaid Payment Instruments, whether or not compensation for damage is to be provided to victims for each specific situation in which damage is likely to occur, and the content of and requirements for compensation, if any;

(B) Content of the compensation procedure;

(C) In cases of collaborative services, particulars concerning the sharing of compensation between the Issuer of Prepaid Payment Instruments and the business partner (including those who provide compensation to victims);

(D) Inquiry and contact for compensation; and

(E) Standards for disclosure of improper transactions

Note: With regard to the matters specified in (C) above, it is not necessary to notify users of all the contents of the agreement with the business partner with regard to such matters, based on Article 23-2(1)(iii) and Article 23-3(ii) of the Cabinet Office Order, but it should be kept in mind that it is necessary to provide users at least with information on those who provide compensation for the victims.

(iii) Has the Issuer of Prepaid Payment Instruments developed a control environment for appropriately and promptly providing compensation in accordance with the established Compensation Policy (in the case of collaborative services, including a system for cooperation with business partners)?

(iv) Does the Issuer of Prepaid Payment Instruments share necessary information with business partners (if any) and a Certified Association for Payment Service Providers (if it is a member thereof), etc. concerning risks of improper transactions and actual cases thereof, such as inquiries, etc. from users concerning improper transactions?

II-2-9-2 Supervisory Methods and Measures

(1) When a problem is found

With regard to issues and challenges, etc. concerning the response to improper transactions of an Issuer of Prepaid Payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments, by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments, including the viewpoint of protecting the interests of the users, etc., the supervisory authorities shall issue to the Issuer of Prepaid Payment Instruments an order to improve business operations based on Article 25 of the Act. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

(2) When an improper transaction occurs

Upon detecting any improper transaction, the Issuer of Prepaid Payment Instruments is required to make a report to the relevant authorities in the form of “Report on Improper Transaction”.

II-3 Administrative Operations

II-3-1 IT Systems Management

When engaging in the business of issuing Prepaid Payment Instruments, Issuers of Prepaid payment Instruments need to recognize that there is a risk that a user or an Issuer of Prepaid Payment Instruments will incur damage due to a flaw in the computer system such as a failure or malfunction of the system or due to an improper use of the computer (hereinafter referred to as “IT system risk”) and to appropriately manage the system risk.

In particular, regarding IC card-based Prepaid Payment Instruments and Server-type Prepaid Payment Instruments, if the system used by an issuer fails, there is a risk that the amount issued, the amount collected, and the unused balance may fail to be grasped, or that the business of issuing Prepaid Payment Instruments may not be continued, which may cause significant damage to users. Therefore, IT system risk management must be appropriately implemented.

In addition, IT strategies of issuers of IC card-based Prepaid Payment Instruments and Server-based

Prepaid Payment Instruments are critical issues that influence the business model of these issuers in light of recent changes in the financial environment, and there is an increasing need for them to consider management strategies and IT strategies in an integrated manner. From these viewpoints, it is extremely important for the management team of an Issuer of Prepaid Payment Instruments to show leadership, link information technologies to management strategies according to the scale and characteristics of the Issuer of Prepaid Payment Instruments, and thereby have "IT governance," which is a mechanism to create corporate value through such initiatives, work properly and well.

The following viewpoints are given mainly assuming the cases for Issuers of IC-based Prepaid Payment Instruments or Server-type Prepaid Payment Instruments. However, even if an Issuer of Prepaid Payment Instruments fails to respond literally as described hereunder, it is not inappropriate if it is deemed that there is no particular problem from the viewpoint of user protection in light of the scale of such Issuer and the role of computer systems in its business of issuing Prepaid Payment Instruments.

In addition, even in the case of issuing magnetic- or paper-type Prepaid Payment Instruments, if there is a risk that the business of issuing Prepaid Payment Instruments may be hindered due to an IT system failure, Issuers of these Prepaid payment Instrument need to develop a control environment for the system management as needed.

(Reference) Discussion Paper on Dialogues and Practices Regarding IT Governance at Financial Institutions (June, 2019)

II-3-1-1 Major Supervisory Viewpoints

(1) Recognition of the IT system risk

(i) Do the management, officers, and employees of the Issuer of Prepaid Payment Instruments fully recognize the importance of IT system risks in the business of issuing Prepaid Payment Instruments and conduct periodic reviews and formulate basic policies for risk management as needed, according to the role played by IT system in such business?

(ii) Has the management team recognized that prevention of an IT system failure and cybersecurity incident (hereinafter referred to as "IT system failures, etc.") and efforts for speedy recovery on the occurrence of such IT system failures, etc. is an important issue for the management, and developed an appropriate control environment?

Note:"Cybersecurity incidents" refer to instances of cybersecurity being threatened by so-called "cyberattacks", including unauthorized intrusion, theft, modification, and destruction of data, failure or malfunction of information systems, and execution of illegal computer programs and DDoS attacks, committed via the Internet through malicious use of information communication networks and information systems.

(iii) Has the management team appointed an officer who oversees and manages IT systems, fully recognizing the importance of the IT system risk? It is desirable that the officer in charge of IT systems should be a person who has sufficient knowledge and experience in IT systems to properly pursue the relevant operations.

(iv) Has the management team specified their responsibilities to assume and response to take in case of crisis where an IT system failure, etc. occurs?

Also, do they conduct drills giving directions by themselves and ensure the effectiveness thereof?

(2) Control environment for managing IT system risk

(i) Has the management team established the risk management environment while fully

understanding that, due to highly networked computer systems, if risk becomes apparent, the impact would cause chain reaction, spread widely and seriously, and adversely affect the management of the Issuer of Prepaid Payment instruments? In addition, in cases where the Issuer of Prepaid Payment Instruments conducts the business of issuing Prepaid Payment Instruments as part of multiple integrated services, has the Issuer of Prepaid Payment Instruments developed a risk management system covering the overall system of these multiple services?

(ii) Has the Issuer of Prepaid Payment Instruments established the basic policy for managing the IT system risk? Does the basic policy for managing the IT system risk contain the security policy (a basic policy for proper protection of information assets of an organization) and the policy on outsourced contractors?

(iii) Is the Issuer of Prepaid Payment Instruments basing the details of its control environment for managing the IT system risk on criteria that allow it to judge objective levels of its details?

Also, does the Issuer of Prepaid Payment Instruments revise, on a continual basis, its control environment for managing the IT system risk according to identification and analysis of IT system failures, etc., results of implementation of risk management, progress of technology, etc.?

(3) Assessment of the IT system risk

(i) Does the division in charge of managing the IT system risk recognize and assess risks periodically and in a timely manner by recognizing that risks are becoming diversified due to changes in the external environment, such as seen in the examples of IT system failures, etc. induced by large-scale transactions as a result of increased customer channels and efforts to enhance information networks that bring more diverse and broad-based impact?

Also, does it take sufficient measures to address the risks that have been identified?

If the Issuer of Prepaid Payment Instruments has sophisticated and complex information systems that are linked to various services and systems (including those provided by outside operators), are the following included in the IT system risk?

- Risks arising from the use of diverse services and systems; and
- Risks associated with linking with a variety of services and systems, including responding to a surge in transactions.

In cases where transactions are expected to increase sharply, does the Issuer of Prepaid Payment Instruments take necessary measures by coordinating in advance the number of expected transactions with other companies that use the linked IT systems?

(ii) Does the division in charge of managing the IT system risk identify and manage the upper limit of the transactions through the computer system, such as the number of transactions possible per day, for example? And does it consider system and administrative measures for cases where the transactions exceed the upper limit?

(iii) Do the departments in charge of users cooperate with the division in charge of managing the IT system risk at the time of introduction of the services and/or at the time of any change in the contents and methods thereof? And does the department in charge of managing the IT system risk evaluate a relevant IT system regardless of whether the system is newly developed or not?

(4) Management of information security

(i) Has the Issuer of Prepaid Payment Instruments developed a policy, prepared organizational readiness, introduced internal rules, and developed an internal control environment in order to appropriately manage information assets? Also, is it making continuous efforts to improve its information security control environment through the PDCA cycle, taking notice of illegal incidents or lapses at other companies?

(ii) Does the Issuer of Prepaid Payment Instruments manage information security by designating individuals responsible for it and clarifying their roles/responsibilities in efforts to maintain the confidentiality, integrity, and availability of information? Also, are the individuals responsible for information security tasked to handle the security of IT system, data, and network management?

(iii) Does the Issuer of Prepaid Payment Instruments take measures to prevent unauthorized use of computer systems, unauthorized access, and intrusion by malicious computer programs such as computer viruses?

(iv) Does the Issuer of Prepaid Payment Instruments comprehensively identify, grasp and manage important information on users for which it should be responsible?

Does the scope of important information to be identified by the Issuer of Prepaid Payment Instruments cover information and data used in the course of business operations or stored in IT systems and kept by outsourced contractors and include data, for example, as listed below?

- Data stored in the areas within the IT system that are not used in ordinary operations;
- Data output from the IT system for analyzing system failures; and
- Data, etc. transferred to outsourced contractors and partners

(v) Does the Issuer of Prepaid Payment Instruments assess importance and risks regarding important user information that has been identified?

Also, has it developed rules to manage information, such as those listed below, in accordance with the importance and risks of each type of information?

- Rules to encrypt or mask information;
- Rules for utilizing information; and
- Rules on handling data storage media, etc.

(vi) Has the Issuer of Prepaid Payment Instruments introduced measures to discourage or prevent unauthorized access, unauthorized retrieval, data leakage, etc. such as those listed below, for important user information?

- Provision of access rights limited to the extent necessary according to the respective roles of the divisions and sites (including overseas ones)
- Provision of access rights limited to the extent necessary according to the authority of employees
- Storage and monitoring of access logs
- Introduction of mutual checking functions such as by separating the individuals in charge of development and those responsible for operations, or system administrators and system users, etc.

(vii) Has the Issuer of Prepaid Payment Instruments introduced rules for controlling confidential information, such as encryption and masking? Also, has it introduced rules regarding the management of encryption programs, encryption keys, and design specifications for encryption programs, etc.?

Note that “confidential information” refers to any information that may cause damage or

loss to users if it is disclosed or stolen, such as PINs, passwords, credit card information, etc.

(viii) Does the Issuer of Prepaid Payment Instruments give due consideration to the necessity of holding/disposing of, restricting access to, and taking outside, confidential information, and treat such information in a stricter manner?

(ix) Does the Issuer of Prepaid Payment Instruments periodically monitor its information assets to see whether they are managed properly according to management rules, etc., and review the control environment on an ongoing basis?

(x) Does the Issuer of Prepaid Payment Instruments conduct security education (including securities education at outsourced contractors) to all officers and employees in order to raise awareness of information security?

(xi) Has the Issuer of Prepaid Payment Instruments taken measures in case of data loss, such as taking backup of data on a regular basis?

(5) Cyber security management

(i) Has the management team developed a necessary control environment upon recognizing the importance of cybersecurity amid increasingly sophisticated and cunning cyberattacks?

(ii) Has the Issuer of Prepaid Payment Instruments introduced systems to maintain cybersecurity, such as those listed below, in addition to making the organization more secure and formulating internal rules?

- Monitoring systems against cyberattacks;
- Systems to report cyberattacks and public-relation system when attacks occur;
- Emergency measures by an in-house Computer Security Incident Response Team (CSIRT) and systems for early warning; and
- Systems of information collection and sharing through information-sharing organizations, etc.

(iii) Has the Issuer of Prepaid Payment Instruments introduced a multi-layered defense system against cyberattacks that combines security measures respectively for inbound perimeter control, internal network security control, and outbound perimeter control?

- Security measures for inbound perimeter control (e.g. installation of a firewall, web application firewall, anti-virus software, unauthorized intrusion detection system, unauthorized intrusion prevention system, etc.);
- Internal measures (e.g. proper management of privileged IDs and passwords, deletion of unnecessary IDs, monitoring of execution of specific commands, securing of production systems (between servers) (packet filtering and encryption of communications), separation of networks in development environments (including test-phase environments) and use-phase environments, separation of network segments according to usage purposes, etc.)
- Security measures for outbound perimeter control (e.g. retrieval and analysis of communication/event logs, detecting/blocking inappropriate communication, etc.)

(iv) Has the Issuer of Prepaid Payment Instruments taken measures such as those listed below to prevent damage from expanding when cyberattacks occur?

- Identifying IP addresses of attackers, and blocking off attacks;
- Functions to automatically decentralize accesses against DDoS attacks; and
- Temporary suspension, etc. of the entire system or part thereof

(v) Are necessary measures introduced for vulnerabilities in the IT system, such as updating of

the operating system and application of security patches, in a timely manner?

(vi) Does the Issuer of Prepaid Payment Instruments, as part of cybersecurity measures, assess its security levels periodically by using network intrusion tests or relevant vulnerability scanning, etc. and make efforts to improve security?

(vii) When conducting non-face-to-face transactions using the Internet and other means of communication, has the Issuer of Prepaid Payment instruments introduced an appropriate authentication method that matches the risks of transactions, such as the following?

Also, in light of changes in the domestic and overseas environment and the occurrence of accidents and incidents, does the Issuer of Prepaid Payment instruments recognize and evaluate risks periodically and in a timely manner and review the certification methods as needed?

- Authentication methods that do not rely solely on fixed IDs and passwords, such as multi-factor authentication that combines effective elements such as variable passwords, biometrics, and electronic certificates;
- Transaction authentication through multiple channels, such as by using, for example, a device that is different from a PC or smart device used for transactions;
- Adoption of a trading password that is different from the login password (Note that the same password cannot be set.); and
- Terminal authentication function that allows only specific terminals to be used, etc.

Note: It should be kept in mind that it is necessary to introduce a robust authentication method for registering and changing information used for authentication, such as telephone numbers, email addresses, and passwords.

(viii) When conducting non-face-to-face transactions using the Internet and other means of communication, has the Issuer of Prepaid Payment Instruments taken following anti-fraud measures, for example, corresponding to the business?

- Interrupting communications from invalid IP addresses;
- Taking measures to encourage users to introduce and update security software that allows them to detect and remove viruses, etc.;
- Introduction of a system to detect unauthorized log-ins, abnormal transactions, etc. and promptly notify such anomalies to users who can be contacted;
- Suspending the use of IDs that have been confirmed to be used for unauthorized purposes;
- Displaying the last login (logoff) date and time on the screen; and
- Notifying users at the time of transaction, etc.

(ix) Has the Issuer of Prepaid Payment Instruments developed contingency plans against potential cyberattacks? And does it conduct exercises and review such plans? Also, does it participate in industry-wide exercises as necessary?

(x) Has the Issuer of Prepaid Payment Instruments formulated plans to train and develop personnel responsible for cybersecurity and implemented them?

(6) IT system planning/development/management

(i) Does the Issuer of Prepaid Payment Instruments make continuous efforts to identify risks inherent in the current IT system and make investment in maintaining such efforts and eliminating risks in a planned manner?

When planning and developing IT system, it is desirable to clarify the IT system strategy policy as a part of the management strategy and to formulate a medium to long-term development plan approved by the management team.

(ii) Are rules to authorize plans, development, and transitions of IT system development projects clearly established?

(iii) Does the Issuer of Prepaid Payment Instruments appoint and assign a responsible person to each IT system development project and manage the project according to the development plan?

(iv) When conducting non-face-to-face transactions using the Internet and other means of communication, are the following security requirements included in the rules related to the system design/development stage?

- Clarifying specific security requirements;
- Taking measures to prevent any vulnerability in the system such as secure coding; and
- When linking with other companies' systems, the system should have a security design considering not only the linked part but also the entire service, etc.

(v) When linking with other companies' systems, or when a large number of users are expected to use the system of Prepaid Payment Instruments, has the Issuer of Prepaid Payment Instruments formulated rules and policies, etc., including the following viewpoints, and implemented them appropriately in order to ensure the quality of the entire system?

- Establishing test implementation policies to ensure quality;
- Formulating a plan for performance capacity management of the IT system with a threshold value corresponding to surging transaction based on examples of other companies (including cases where the number of temporary transactions is expected to increase, such as large-scale sales promotion activities);
- Setting monitoring items, monitoring of load conditions, and implementing necessary control, taking into consideration the limits of performance and capacity of various resources; and
- Grasping system limits during the IT system development

(vi) In developing IT systems, does the Issuer of Prepaid Payment Instruments work out a test plan and conduct a test in an appropriate and sufficient manner, such as by involving departments in charge of users in it?

(vii) Has the Issuer of Prepaid Payment Instruments secured personnel who are familiar with the mechanisms of the current IT system and have expertise in system planning, development, and operation management?

It is desirable to formulate and implement a specific plan for the succession of the current IT system structure and development technology, as well as for the development of human resources with expertise.

(7) IT system audit

(i) Does the Internal Audit Department, which is independent from the IT Systems Department, conduct periodic IT system audits by personnel familiar with IT system matters?

Note:External audits may be used instead of internal audits if it is considered more effective to introduce IT system audits by external auditors.

(ii) Does the audit cover all business operations involving the IT system risk?

(iii) Are the results of the IT system audit reported to the management team in a proper manner?

(8) Outsourcing management

(i) Does the Issuer of Prepaid Payment Instruments, in selecting outsourced contractors (including IT system-related subsidiaries), assess them based on selection criteria and give

careful consideration?

(ii) When using external services such as cloud services, does the Issuer of Prepaid Payment Instrument examine risks associated with the services used and take necessary measures?
For example, does it implement the following measures?
- Grasping sites that process and store critical data;
- Reflecting the authority to audit and monitor, etc. in the contract;
- Confirming and evaluating assurance reports, third-party certifications, etc.; and
- Understanding cloud-specific risks, etc.

(iii) Does the Issuer of Prepaid Payment Instruments, in entering an outsourcing contract with an outsourced contractor, set out division of roles and responsibilities with the contractor, supervising authority to audit outsourced work, subcontracting procedures, level of services provided, etc. in the contract? Also, does the Issuer of Prepaid Payment Instruments present to the outsourced contractor rules that its officers and employees are required to adhere to and security requirements, as well as define them in the contract, etc.?

(iv) Is risk management carried out properly in outsourced IT system work (including multi-tiered outsourcing)?
In particular, in cases where the Issuer of Prepaid Payment Instruments outsources its IT system work to two or more contractors, related administrative work becomes complicated and a higher level of risk management is required. In this context, has the Issuer of Prepaid Payment Instruments developed a control environment upon fully understanding such fact?
In cases where IT system-related administrative work is outsourced to contractors, too, does the Issuer of Prepaid Payment Instruments properly manage the risk thereof in the same manner as outsourcing of IT system work?

(v) Does the Issuer of Prepaid Payment Instruments, as an outsourcer, regularly check and monitor to confirm that outsourced work (including multi-tiered outsourcing) is carried out appropriately?
Also, does it take necessary measures not to leave everything to outsourced contractors, by, for example, placing its staff at an outsourced contractor's site to monitor the outsourced work, etc.?
In addition, does the Issuer of Prepaid Payment Instruments put in place a control environment that allows the Issuer, as an outsourcer, to monitor and track the status of user data being processed at outsourced contractors?

(vi) Does the Issuer of Prepaid Payment Instruments audit its important outsourced contractors by its Internal Audit Department or IT system auditors, etc.?

(9) Contingency plan

(i) Has the Issuer of Prepaid Payment Instruments formulated a contingency plan and established arrangements and procedures for dealing with emergencies?
In cases where IT system-related operations are outsourced, has the Issuer of Prepaid Payment Instruments established an emergency system (including communication systems with service providers and system partners) including important outsourced contractors?

(ii) When formulating a contingency plan, does the Issuer of Prepaid Payment Instruments refer to guides that allow it to judge objective levels of its details (such as "Manual for the Development of Contingency Plans in Financial Institutions (Plans for Measures in the Event of Emergencies)" compiled by the Center for Financial Industry Information Systems)?

(iii) When formulating a contingency plan, does the Issuer of Prepaid Payment Instruments assume not only contingencies due to natural disasters but also IT system failures, etc. due to internal or external factors?
Also, does the plan include sufficient risk scenarios assuming the following risks?
- Cyberattack
- Disaster and pandemic
- IT System failure
- Information leakage, etc.

(iv) Does the Issuer of Prepaid Payment Instruments review assumed scenarios in its contingency plan in a timely and appropriate manner by, for example, taking into consideration case studies of IT system failures, etc. at other Issuers of Prepaid Payment Instruments and results of deliberations at the Central Disaster Management Council, etc.?

(v) Does the Issuer of Prepaid Payment Instrument regularly conduct a drill based on its contingency plan?
Is the drill based on the contingency plan conducted at the organization-wide level of the Issuer of Prepaid Payment Instruments? And is it periodically conducted jointly with outsourced contractors and IT system partners according to the degree of importance and risks?
Is the contingency plan reviewed as needed based on training results?

(vi) Has the Issuer of Prepaid Payment Instruments introduced off-site backup IT systems, etc. in advance for important IT systems whose failure could seriously affect business operations? And has it developed a control environment to address disasters or IT system failures, etc. so that normal business operations can be speedily brought back?

(10) Response to IT system failures

(i) Has the Issuer of Prepaid Payment Instruments taken appropriate measures to avoid causing unnecessary confusion among users in the event of IT system failures, etc.?
Also, has it developed a control environment, upon assuming a worst-case scenario in preparation for IT system failures, etc. to take necessary measures accordingly?

(ii) Has the Issuer of Prepaid Payment Instruments clarified reporting procedures and the framework of command and supervision covering outsourced contractors in preparation for IT system failures, etc.?

(iii) Upon occurrence of an IT system failure, etc. that may significantly affect its business operations, is the Issuer of Prepaid Payment Instruments prepared to promptly notify the management team and report the greatest potential risk it poses under the worst-case scenario (for example, if there is a possibility that the failure could gravely affect users, the reporting persons should not underestimate the risk but immediately report the highest risk scenario)?
In addition, is it prepared to launch a task force, have the management team itself issue appropriate instructions and orders, and seek resolution of the issue in a swift manner?

(iv) Has the Issuer of Prepaid Payment Instruments clearly established the support framework for IT system failures, etc. to promptly gather experts having relevant know-how and experience from the IT Systems Department, other departments, or outsourced contractors, for example, through prior registration of these experts?

(v) When an IT system failure, etc. occurs, does the Issuer of Prepaid Payment Instruments disclose the details of the failure, the cause of the failure, and expected recovery time

(Note)? And does it promptly take measures, such as establishing call centers and consultation desks as necessary, and asking the Certified Association for Payment Service Providers for help in responding, if it is a member of the association, in order to properly respond to inquiries from users, etc.?

Also, does the Issuer of Prepaid Payment Instruments clarify arrangements and procedures as to how to provide relevant business departments with necessary information in preparation for IT system failures, etc.?

Note: In addition to posting an announcement on its website, the Issuer of Prepaid Payment Instruments should directly notify users, etc. through smart devices if it is possible.

(vi) Has the Issuer of Prepaid Payment Instruments conducted analysis of causes of IT system failures, etc., investigation about impact until recovery, corrective action, and preventive measures for recurrence in a proper manner?

Also, does it periodically analyze tendencies of factors that have led to such IT system failures, etc. and take measures according to them?

(vii) Has the Issuer of Prepaid Payment Instruments established a systematic framework to minimize impacts of IT system failures, etc. such as a system to bypass the affected part?

Reference: As reference materials relating to the IT system risk, there are, for example, "FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions" (The Center for Financial Industry Information Systems).

II-3-1-2 Supervisory Methods and Measures

(1) When a problem is found

With regard to issues and challenges, etc. concerning the system management of an Issuer of Prepaid Payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments, by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments.

If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

(2) When a system failure has occurred

(i) When it is found that a IT system failure or cybersecurity incident has occurred with respect to the IC-type or Server-type Prepaid Payment Instruments that are separately notified by the Local Finance Bureau, the Issuer of Prepaid Payment Instruments is required to immediately notify the relevant authorities of the fact and then to submit a report in a form of the "Report on Occurrence of IT System Failure, etc." (Appended Form 1-1).

In addition, the Issuer of Prepaid Payment Instruments is also required to submit a report on recovery of the system and causes of the system failure when they are identified.

Provided, that in cases where the causes are not identified, the Issuer of Prepaid Payment Instruments must report the actual situation within one month from the occurrence of the IT system failure.

Upon receipt of a report from the Issuer of Prepaid Payment Instruments, Local Finance Bureaus shall immediately contact the relevant division of the Financial Services Agency.

Note: IT system failures, etc. that must be reported

Failure or trouble that occurred in IT systems and devices (both hardware and software) currently used by an Issuer of Prepaid Payment Instruments for whatever reason and;

(A) that caused or may cause suspension of issuance or use, etc. of Prepaid Payment Instruments; or

(B) that may otherwise be deemed similar to the above in the course of business.

However, this reporting requirement does not apply in cases where, even when a part of an IT system or device is failed or troubled, there is no substantial impact or damage because the affected part is able to be promptly replaced by another system or device (e.g. cases where even when Prepaid Payment Instruments become unavailable at some stores due to an IT system failure, users can use them at other or nearby stores.)

Even though a failure or trouble does not actually occur, an Issuer of Prepaid Payment Instruments is required to make a report when the users or business operations are affected or highly likely to be affected because it receives an advance notice of cyberattack or it has found a cyberattack in its IT system.

(ii) The supervisory authorities shall require the Issuer of Prepaid Payment Instruments to submit an additional report pursuant to Article 24 of the Act, as needed, and if it is found that the Issuer of Prepaid Payment Instruments has a serious problem, the supervisory authorities shall issue an order to improve business operations pursuant to Article 25 of the Act.

(iii) In particular, when a major IT system failure, etc. has occurred, or when it takes considerable time for the Issuer of Prepaid Payment Instruments to solve the causes of the failure, the supervisory authorities, while watching the Issuer of Prepaid Payment Instruments activate its contingency plan including general announcement of the details of the failure to the public and responses to users at stores, etc., requires the Issuer of Prepaid Payment Instruments to promptly identify the causes and asks for prompt recovery, and requires a prompt report pursuant to Article 24 of the Act.

(3) Responses at the time of IT system update and integration, etc.

When an Issuer of Prepaid Payment Instruments updates or integrates important IT systems, the supervisors require the Issuer of Prepaid Payment Instruments to submit a report based on Article 24 of the Act as needed, and confirm plans and progress, as well as the appropriateness and effectiveness of project management, and then take actions such as issuing an order for business improvement based on Article 25 of the Act if significant problems are found.

(4) Response to outsourced contractors

When it deems necessary, for example, in cases where there is a concern that outsourced contractors fail to properly operate IT systems work that has been outsourced, the supervisory authorities takes actions under II-3-3-2 hereof.

II-3-2 Administrative Risk Management

Administrative risk refers to the risk that an Issuer of Prepaid Payment Instruments incurs a loss due to its officers and/or employees failing to perform accurate administrative work or due to their problematic conducts or wrongful acts. Issuers of Prepaid Payment Instruments need to strive to ensure their reliability and creditworthiness by properly developing an internal control environment regarding administrative risk and maintaining the soundness and appropriateness of their business operations. The following points, for example, shall be taken into consideration.

Even if an Issuer of Prepaid Payment Instruments fails to respond literally as described hereunder, it is not inappropriate if it is deemed that there are no particular problems from the viewpoint of protecting the interests of users of Prepaid Payment Instruments in light of the scale and characteristics of such Issuer of Prepaid Payment Instruments.

II-3-2-1 Major Supervisory Viewpoints

(1) Control environment for managing administrative risk

(i) Has the Issuer of Prepaid Payment Instruments developed an appropriate control environment for managing administrative risk based on the understanding that such risk is involved in all business operations?

(ii) Has the Issuer of Prepaid Payment Instruments implemented specific measures to reduce administrative risk based on the recognition of the importance of reducing such risk?

(iii) Has the Issuer of Prepaid Payment Instruments developed a control environment wherein the division in charge of administrative work is able to perform the internal check-and-balance function sufficiently? Also, has the Issuer of Prepaid Payment Instruments established rules and regulations regarding administrative work and processes?

(iv) Does the Issuer of Prepaid Payment Instruments treat important legal compliance issues as a company-wide legal compliance issue rather than processing them as a mere administrative problem?

(2) Administrative risk management by internal audit function

Does the Internal Audit Department properly conduct internal audits in order to examine the control environment for managing administrative risk?

(3) Control environment for managing administrative risk in business offices

Has the division in charge of managing administrative risk at headquarters taken measures for checking business offices' control environment for managing administrative risk?

II-3-2-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning control environment for administrative risk management of an Issuer of Prepaid Payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment

Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-3-3 Outsourcing

Even when an Issuer of Prepaid Payment Instruments outsources part of its business to a third party (including multi-tiered outsourcing), the Issuer is not exempted from the final responsibility pertaining to such outsourced work. Therefore, in order to ensure the protection of users and the sound and appropriate operation of the business, it is necessary to pay attention to the following points, for example, depending on the nature of the business of the Issuer of Prepaid Payment Instruments. It should be noted that the following points are only general points of view, and additional verification may be required, depending on the content of the outsourced work.

II-3-3-1 Major Supervisory Viewpoints

(i) Has the Issuer of Prepaid Payment Instruments established internal rules, etc. stipulating criteria for selecting contractors or measures to be taken when outsourcing risk appears, and disseminated them company-wide through internal training, etc. so that its officers and employees properly handle cases in accordance with such internal rules, etc.?

(ii) Has the Issuer of Prepaid Payment Instruments taken appropriate measures regarding the development of a legal compliance system at the outsourced contractor, such as issuing necessary instructions? In addition, has the Issuer of Prepaid Payment Instruments taken measures to ensure that outsourcing does not hinder the performance of obligations to supervisory authorities regarding inspections, reporting orders, submission of records, etc.?

(iii) Has the Issuer of Prepaid Payment Instruments made it clear that the outsourcing of business operations does not cause any change in the contractual rights and obligations involving it and its users and that the users continue to have the same rights as if the business operations were conducted by the Issuer of Prepaid Payment Instruments itself?

Note:Outsourcing includes cases where an Issuer of Prepaid Payment Instruments is deemed to substantially outsource its business to an external contractor even if a formal contract is not concluded or where the outsourced work is performed overseas.

(iv) In the case of outsourcing the operation relating to cash payment and receipt with users, when the outsourced contractor receives and pays cash from or to users, has the Issuer of Prepaid Payment Instruments taken measures to appropriately identify increases and decreases in the unused balance pertaining to the receipt and payment of cash?

(v) Has the Issuer of Prepaid Payment Instruments developed a control environment that prevents users from suffering inconveniences if the Issuer of Prepaid Payment Instruments cannot be provided with the services agreed under the outsourcing contract with its outsourced contractor?

(vi) When outsourcing the handling of information of individual users to an external contractor, has the Issuer of Prepaid Payment Instruments taken the measures to supervise the outsourced contractor as necessary and appropriate measures to prevent such information from being leaked, lost, or damaged based on Article 10 of the Financial Sector Personal Information Protection Guidelines and III of the Practice Guidelines?

(vii) With regard to the management of outsourced contractors, does the Issuer of Prepaid Payment Instruments clarify the responsible division and confirm that outsourced contractors are properly managing information related to users, such as by monitoring on a periodic or as-needed basis how business operations are being conducted at outsourced contractors?

(viii) Has the Issuer of Prepaid Payment Instruments confirmed that outsourced contractors have systems in place to take appropriate actions and to promptly report to the Issuer of Prepaid Payment Instruments in the event that information is leaked, lost, or damaged at outsourced contractors?

(ix) Does the Issuer of Prepaid Payment Instruments restrict the access right by outsourced contractors to the information related to users possessed by the Issuer of Prepaid Payment Instruments to the extent necessary according to the nature of the outsourced business?

On that basis, does the Issuer of Prepaid Payment Instruments check whether the officers and employees at outsourced contractors to whom access rights are given have been defined, along with the scope of their access rights?

Furthermore, does the Issuer of Prepaid Payment Instruments confirm that the access rights are being managed thoroughly at outsourced contractors on a periodic or as-needed basis, such as by checking how the access rights are used (including crosschecking authorized persons with actual users) in order to prevent the access rights assigned to certain people from being used by others?

(x) In cases of multi-tiered outsourcing, does the Issuer of Prepaid Payment Instruments check whether the outsourced contractor is adequately supervising its subcontractors and other business operators? In addition, does the Issuer of Prepaid Payment Instruments directly supervise such subcontractors and other business operators as needed?

(xi) With regard to complaints, etc. pertaining to the outsourced service, has the Issuer of Prepaid Payment Instruments developed an appropriate complaint consultation system, such as a system to accept direct communication from users to the Issuer of Prepaid Payment Instruments, who is the entrustor of such service?

II-3-3-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning outsourcing of an Issuer of Prepaid Payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

Note: Interviews shall basically be conducted with an Issuer of Prepaid Payment Instruments who

outsourced services in order to understand the facts of a case, etc. However, in the light of the urgency and seriousness of the case, the supervisors shall consider having an interview with outsourced contractors in parallel as needed.

When having an interview with an outsourced contractor, the supervisors shall ask the Issuer of Prepaid Payment Instruments, who has outsourced its service to the outsourced contractor, to attend the interview as needed.

II-3-4 Refunds of Prepaid Payment Instruments

When supervising Issuers of Prepaid Payment Instruments in terms of control environment for refund of Prepaid Payment Instruments, the following points, for example, shall be taken into consideration.

II-3-4-1 Major Supervisory Viewpoints

(i) Refunds pursuant to Article 20(1) of the Act

(A) Has the Issuer of Prepaid Payment Instruments taken proper measures in order to ensure that the particulars prescribed in the items of Article 20(2) of the Act are properly posted at all of its business offices or offices and member shops, for example, by notifying the member shops of the content and period of such notice posting, as well as checking the notice posting status? When the public notice is made via daily newspapers, does such public notice cover all the prefectures in which the facilities where the Prepaid Payment Instruments subject to the procedure for the refund can be used are located? (Note)

In the cases prescribed in Article 41(4) of the Cabinet Office Order, the Issuer of Prepaid Payment Instruments must, in lieu of the notice posting at its business offices or offices and member shops, provide the users with information concerning the predetermined matters at least by the same method as the Issuer usually uses in performing its obligation to provide information prescribed in Article 13(1) of the Act, among those under the items of Article 21(2) of the Cabinet Office Order.

(B) It is preferable that when the Issuer of Prepaid Payment Instruments intends to give a refund, the Issuer of Prepaid Payment Instruments should take the following measures from the viewpoint of protecting users.

a) Dissemination of information on termination of use

When an Issuer of Prepaid Payment Instruments has decided the day on which to terminate the use of the Prepaid Payment Instruments, the Issuer should promptly notify users thereof by posting it on its own website or via a poster at its member shops, etc. in order to secure a certain period so that the users have opportunities to use the Prepaid Payment Instruments.

b) Period for making claims for refund

The 60-day period specified by the relevant laws is the minimum period for making claims for refund. The Issuer of Prepaid Payment Instruments should set a period for making claims for refund that is long enough to secure opportunities for users to receive the refund.

c) Method for disseminating how to refund

In addition to the methods required by the laws, an Issuer of Prepaid Payment Instruments should post the relevant information, for example, on its own website, websites of member shops, those of the industrial associations, etc. to which it belongs, the website of the Certified Associations for Payment Service Providers, and on the

website of the National Consumer Affairs Center of Japan.

From the viewpoint of securing the effectiveness of the refund, it should be kept in mind that the Issuer of Prepaid Payment Instruments should make public the information on termination of use and set the period for making claims for refund and the method for disseminating such information not in a uniform and mechanical manner, but in an appropriate manner upon considering the characteristics of the Prepaid Payment Instruments subject to the refund, including the issuance scale (unused balance, number, etc.) and the nature of use thereof.

(C) Have all the users who made claims for refund received the refund without exception?

Note 1: The term "termination of use" refers to the discontinuation of the business of issuing Prepaid Payment Instruments in whole or in part (excluding the cases where said business was succeeded to any third party by inheritance, transfer of business, merger or company split, or for other reasons).

Note 2: If it is not deemed that an Issuer of Prepaid Payment Instruments has taken sufficient measures prescribed in Article 20(2) of the Act in light of the implementation status of public notice and posting at business offices or other offices and member shops, it should be noted that the refund procedure prescribed in Article 20(1) of the Act cannot be deemed to have been properly implemented and that Prepaid Payment Instruments for which no refund was actually made during that period cannot be deducted from the unused balance.

(ii) Refunds pursuant to Article 20(5) of the Act

(A) In consideration that refunds cannot be made even during the period if the total amount of refunds exceeds the amount specified in Article 42 of the Cabinet Office Order, has the Issuer of Prepaid Payment Instruments developed a control environment for preventing refunds from exceeding the upper limit specified by laws and regulations by, for example, keeping refund records during the period as necessary?

(B) When responding to claims for refund from users based on Article 20(5) of the Act and Article 42(1)(i) or (ii) of the Cabinet Office Order, has the Issuer of Prepaid Payment Instruments appropriately explained the refund procedure to users? For example, has it provided users with an explanation that could mislead the user into believing that "refund is always possible"?

(C) When making an application for approval of refund pursuant to Article 20(5) of the Act and Article 42(1)(iv) of the Cabinet Office Order, has the Issuer of Prepaid Payment Instruments confirmed in the balance sheet, etc. that it has sufficient financial resources to cover the refund of all issued Prepaid Payment Instruments, from the viewpoints of preventing any shortage of financial resources as a result of the refund and of ensuring that holders of Prepaid Payment Instruments other than those subject to refund will receive a sufficient refund?

Note: As an example of cases where Issuers of Prepaid Payment Instruments make an application for approval of refund, there are cases where Server-type Prepaid Payment Instruments suffered cyber attacks and are subject to a continuing risk of unauthorized use.

II-3-4-2 Supervisory Methods and Measures

If, as a result of examining the content, etc. of the notification under Article 41(4) and (5) of the Cabinet Office Order, there is any doubt as to whether the refund procedure under Article 20(1) of

the Act has been properly carried out, the supervisors shall confirm that the refund procedure has been properly carried out by collecting a report pursuant to Article 24 of the Act, as necessary, before granting approval for the recovery of the security deposit for issuance pursuant to Article 18(iv) of the Act.

Also, with regard to issues and challenges, etc. concerning refunds of Prepaid Payment Instruments by an Issuer of Prepaid Payment Instruments, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users of Prepaid Payment Instruments, the supervisory authorities shall issue an order to improve business operations based on Article 25 of the Act to the Issuer of Prepaid Payment Instruments. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 26 or 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-3-5 Management of Member Shops (for Issuers of Prepaid Payment Instruments for Third-Party Business only)

With respect to Issuers of Prepaid Payment Instruments for Third-Party Business, since it is their member shops that provide users with goods and services, it is necessary to confirm that the contents of goods and services sold and provided by the member shops do not violate public order and morals, in order to prevent improper use of Prepaid Payment Instruments.

The term “harmful to or pose any risk of being harmful to public order or morals” stipulated in Article 10(1)(iii) of the Act includes not only cases where there is strong maliciousness such as criminal acts, but also cases where it lacks or is likely to lack social appropriateness. It should be fully noted that it is necessary to manage member shops appropriately in order that these cases are not included.

In addition, it is necessary to take measures to appropriately make payments to member shops from the viewpoint of ensuring the credibility of Prepaid Payment Instruments, as a means of settlement.

II-3-5-1 Major Supervisory Viewpoints

(i) When concluding a member shop contract, does the Issuer of Prepaid Payment Instruments confirm whether or not the counterparty is engaging in suspicious business in light of public order and morals?

(ii) If it is found that there is a problem in the business of a member shop in light of public order and morals after the conclusion of the member shop contract, is it possible to promptly cancel the contract?

(iii) Has the Issuer of Prepaid Payment Instruments developed a control environment that enables it to identify any significant change in the matters confirmed at the time of the conclusion of a member shop contract, such as requiring the member shop to report any significant change in the details of its goods and services sold or provided to users after the conclusion of the member shop contract?

(iv) Does the Issuer of Prepaid Payment Instruments require each member shop to report on the use of Prepaid Payment Instruments at regular intervals? Also, does it have a control environment in which a department different from the department that manages the usage records of member shops verifies the accuracy of the reported payment amounts?

II-3-5-2 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning the management of member shops by an Issuer of Prepaid Payment Instruments for Third-Party Business, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Issuer of Prepaid Payment Instruments for Third-Party Business, by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 24 of the Act, based on the viewpoints mentioned above.

In addition, if the Issuer of Prepaid Payment Instruments for Third-Party Business is found to have serious problems from the viewpoint of ensuring sound and appropriate operation of the business of issuing Prepaid Payment Instruments including the viewpoint of protecting the interests of the users and the member shops of Prepaid Payment Instruments, the supervisory authorities shall issue to the Issuer of Prepaid Payment Instruments for Third-Party Business an order to improve business operations based on Article 25 of the Act If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 27 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-4 Special Provisions concerning Succession of the Business of Issuing Prepaid Payment Instruments for Own Business

When supervising the succession of the business of issuing Prepaid Payment Instruments for Own Business, the following points, for example, should be taken into consideration.

II-4-1 Major Supervisory Viewpoints

(i) If the reason for succession of the business of issuing Prepaid Payment Instruments for Own Business is other than inheritance or merger, is it ensured that the successor fulfills the deposit obligation required by laws and regulations?

Note:If the successor does not succeed to the security deposit for issuance, etc. from the predecessor, it is necessary to confirm with the successor about the schedule for its security deposit for issuance.

(ii) In light of the content of goods and services provided by the successor, is it ensured that users are able to enjoy the same convenience as before succession of the issuing business?

II-4-2 Supervisory Methods and Measures

When a written notification has been submitted pursuant to Article 30(2) of the Act, the supervisory authorities shall confirm whether it is ensured that the successor will fulfill the deposit obligation required by laws and regulations and whether the successor has the capability to provide users with goods and services similar to those provided by the predecessor, and shall issue an order to improve business operations to make a security deposit for issuance to the successor if a material problem is found in terms of ensuring sound and appropriate management of the business of issuing Prepaid

Payment Instruments, including protection of the interests of the users.

II-5 Basic Views on Persons Engaged in the Business of Issuing Prepaid Payment Instruments in Foreign Countries

II-5-1 No Soliciting of Prepaid Payment Instruments Issued in Foreign Countries

A person engaging in the business of issuing Prepaid Payment Instruments in a foreign state may not solicit a person in Japan for Prepaid Payment Instruments issued by that person in the foreign state.

II-5-2 Cross-Border Transactions Using the Internet, etc. Conducted by Persons Engaged in the Business of Issuing Prepaid Payment Instruments in Foreign Countries

An act of posting an advertisement, etc. by a person engaging in the business of issuing Prepaid Payment Instruments in a foreign state on its website, etc. with regard to the Prepaid Payment Instruments issued by said person is, in principle, deemed as "act of soliciting/solicitation."

Provided, however, that this shall not be considered "soliciting/solicitation" directed to a person in Japan as long as reasonable measures, including the measures set forth below, are taken so as not to result in purchase of the relevant Prepaid Payment Instruments by a person in Japan.

(1) Disclaimer

It clearly states that no person in Japan can purchase Prepaid Payment Instruments issued in the foreign state (hereinafter referred to as the "disclaimer").

The following points should be taken into consideration when determining whether the above measures have been taken sufficiently.

(i) No particular operation of computer or device other than viewing the advertisement is required for reading and understanding the disclaimer.

(ii) The disclaimer must be indicated in language reasonably deemed to be readable and understandable for those in Japan who are accessing the website.

(2) Measures to prevent transactions

Measures have been taken to prevent persons in Japan from purchasing Prepaid Payment Instruments issued in said foreign state.

The following points should be taken into consideration when determining whether the above measures have been taken sufficiently.

(i) At the time of a sale, the seller has gone through the procedure to confirm the residence of the purchaser by having the purchaser present his/her address, mailing address, e-mail address, payment method, and other information.

(ii) In cases where there are reasonable grounds to believe that it is clearly an act of purchasing Prepaid Payment Instruments issued in a foreign state by a person in Japan, the seller takes care not to accept orders from the person in Japan.

(iii) The seller has been attentive in order not to conduct any act of inducing persons in Japan to purchase Prepaid Payment Instruments issued in a foreign state, including establishing call centers for users in Japan or linking websites targeted at persons in Japan.

In addition, the measures listed above are merely examples, and if equivalent or superior measures are taken, posting of advertisements, etc. shall not be deemed to be an act of "soliciting/solicitation" for persons in Japan.

(3) In cases where reasonable measures described above are not taken, since the posting of advertisement, etc. is highly likely to be deemed as the act of "soliciting/solicitation" of Prepaid Payment Instruments issued in a foreign state for persons in Japan, the person engaging in the business of issuing Prepaid Payment Instruments in said foreign state should prove that it has not conducted any act of selling Prepaid Payment Instruments issued in the foreign state with persons in Japan, including any solicitation thereof.

III. Points of Attention regarding Administrative Processes for Inspection and Supervision of Issuers of Prepaid Payment Instruments

III-1 Basic Views and General Administrative Processes, etc.

III-1-1 Basic Views on Inspection and Supervision

The purpose of inspecting and supervising an Issuer of Prepaid Payment Instruments is to enforce registration and provide other necessary measures with respect to the issuance, etc. of Prepaid Payment Instruments in order to ensure the appropriate provision of payment services, and protection of the users, etc. thereof, and to promote the provision of those services, thereby contributing to the improvement of the safety, efficiency, and convenience of the payment and settlement system (see Article 1 of the Act).

To accomplish the purpose of such inspection and supervision, the supervisory authorities need to make continuous responses commensurate with the scale and characteristics of each Issuer of Prepaid Payment Instruments.

For this, in conducting the inspection and supervisory affairs of Issuers of Prepaid Payment Instruments, it is essential to first understand the policies of how each Issuer of Prepaid Payment Instruments intends to address issues and challenges in developing business models and establishing compliance management and risk management systems, and then to accurately understand how these policies are implemented, what governance systems are operated for such implementation, what potential risks or problems lurk, and how Issuers of Prepaid Payment Instruments recognize and respond to their respective risks and problems.

In order to respond to important issues from the perspective of overall management, to ensure the soundness and appropriateness of the business of an Issuer of Prepaid Payment Instruments and the protection of users, etc., and to contribute to the stability of the fund settlement system, etc., each Issuer of Prepaid Payment Instruments itself needs to transform its management structure so that it can work on continuous improvement toward the best practices on its own without being pointed out by the supervisory authorities.

The supervisory authorities will encourage each Issuer of Prepaid Payment Instruments to pursue its efforts in seeking better practices through continuous monitoring through fact-finding and dialogue.

Furthermore, if, in the course of such monitoring activities, the supervisors find, in connection with the business operations of the Issuer of Prepaid Payment Instruments, that there is the fact that the interests of users are harmed or that the business will not be improved only by voluntary efforts of the Issuer of Prepaid Payment Instruments, the supervisors shall consider whether to issue an order to improve business operations pursuant to Article 25 of the Act or to impose other administrative disposition (as explained in III-3).

(1) Ensuring adequate communication with the Issuer of Prepaid Payment Instruments

In inspecting and supervising an Issuer of Prepaid Payment Instruments, it is important to

adequately gather and analyze information about the business operations of the Issuer of Prepaid Payment Instruments and to respond appropriately and in a timely manner. For this reason, the supervisory authorities should, in addition to obtaining reports from Issuers of Prepaid Payment Instruments, endeavor to closely communicate with them and collect information on a day-to-day basis under sound and constructive tension with Issuers of Prepaid Payment Instruments. More specifically, it is necessary to ensure daily communication with Issuers of Prepaid Payment Instruments through regular and timely interviews and exchanges of opinions with various officers and employees thereof, including the management team, outside directors, and persons in charge of internal audits, and to endeavor to grasp not only financial information but also various information on management.

(2) Respect for voluntary efforts of Issuers of Prepaid Payment Instruments

While each Issuer of Prepaid Payment Instruments, as a private company, makes management decisions at its own risk and responsibility, the role of the supervisory authorities is to review such decisions based on relevant laws and regulations and to encourage each of them to resolve problems by its own efforts and resources. With this role firmly in mind, the supervisors must pay due regard to the initiatives of Issuers of Prepaid Payment Instruments in their business operations throughout supervisory processes.

(3) Ensuring efficient and effective inspection and supervisory

From the viewpoint of making effective use of limited resources of the supervisory authorities and Issuers of Prepaid Payment Instruments, it is necessary to conduct inspection and supervisory activities efficiently and effectively while taking into consideration the scale and characteristics of Issuers of Prepaid Payment Instruments. Therefore, when the supervisors ask an Issuer of Prepaid Payment Instruments to submit reports or other documents, the scope of such documents must be limited to the extent truly necessary for the relevant supervisory processes. More importantly, the supervisors must continue efforts to enhance efficiency and effectiveness of supervisory services; the necessity of the supervisory processes currently adopted and their methodologies should be constantly reviewed and supervisory processes should be redesigned whenever necessary.

The content of the reports previously obtained from Issuers of Prepaid Payment Instruments and the procedures for requesting submission of reports or documents are reviewed once every year to streamline such procedures and reduce paperwork burdens of Issuers of Prepaid Payment Instruments. On such occasions, the supervisors should seek opinions of Issuers of Prepaid Payment Instruments about submission requirements.

When requesting a small-scale Issuer of Prepaid Payment Instruments, etc. to submit reports or other documents, the supervisors shall give sufficient consideration of their characteristics so as not to hinder smooth operation of their business.

(4) Active collection of information on Issuers of Prepaid Payment Instruments

In the inspection and supervision of Issuers of Prepaid Payment Instruments, it is important for the supervisors to accurately understand and analyze information on the management of Issuers of Prepaid Payment Instruments, including complaints, etc. from users, etc., and to take appropriate and timely measures for inspection and supervision as necessary.

For this reason, it is necessary to pay attention not only to reports from Issuers of Prepaid Payment Instruments but also to complaints from users, etc., and to actively collect information

through daily and sufficient communication with Certified Associations for Payment Service Providers and Issuers of Prepaid Payment Instruments.

III-1-2 General Supervisory Affairs

(1) Offsite monitoring

Local Finance Bureaus shall endeavor to understand the actual situation of the following matters by examining submitted materials, etc., in cooperation with the relevant divisions of the FSA, as necessary.

When conducting offsite monitoring, the FSA's divisions in charge shall present priority matters for such supervision to the Local Finance Bureaus at the beginning of every fiscal year, and the monitoring shall be conducted based on this.

(i) Basic management (governance) policies, etc.
(ii) Status of internal management
(iii) Status of compliance with laws and regulations
(iv) Status of business operations
(v) Status of internal audits

(2) On-site inspection pursuant to Article 24 of the Act

The supervisors shall conduct on-site inspection pursuant to the Act when it determines that detailed examination is required for verifying the soundness and appropriateness of the current business of an Issuer of Prepaid Payment Instruments, or when it is found necessary on other grounds. In doing so, the supervisors shall always keep in mind what are the most important management issues and what are the underlying causes of these issues, and by holding discussions with the executives of the Issuer of Prepaid Payment Instruments, the supervisors shall endeavor not to reach an easy conclusion but to engage in fundamental discussions on important management and financial administration issues of the Issuer of Prepaid Payment Instruments.

In this regard, see the Basic Procedures for On-Site Inspection, as shown in Exhibit 1. If the supervisors issue a notice of inspection results to an inspected Issuer of Prepaid Payment Instruments, the supervisors shall, within one week after the notice in principle, ask the Issuer of Prepaid Payment Instruments to report its fact-checking of the problems pointed out in the notice, its own analyses of the causes of those problems, planned measures for improvement or remediation, and other comments within one month pursuant to Article 24 of the Act.

(3) Dialogue

Dialogue with an Issuer of Prepaid Payment Instruments is intended to clarify whether any problem that could affect the financial stability and compliance of the Issuer of Prepaid Payment Instruments has occurred or is likely to occur, to review the initiatives of the Issuer of Prepaid Payment Instruments for enhancing business management, or to discuss other issues that are important under the present circumstances or in light of the nature of ongoing problems, as well as the scale and characteristics of the Issuer of Prepaid Payment Instruments.

When holding a dialogue, the supervisors shall avoid imposing their beliefs or hypotheses and endeavor to make the Issuer of Prepaid Payment Instruments feel free to express its views. After hearing its story and grasping its mindset and policies, the supervisors carry out facts-based discussions.

Furthermore, on each occasion of such dialogue session, the supervisors shall make efforts to ensure the continuity of the dialogue, taking into full consideration the communications made

so far between the supervisory authorities and each Issuer of Prepaid Payment Instruments.

(A) If the supervisors determine, based on the facts ascertained, that the Issuer of Prepaid Payment Instruments is highly likely to face a serious problem on compliance, etc., the Issuer of Prepaid Payment Instruments shall, first of all, verify its challenges, the root causes, and the adequacy of remediation measures by itself. Then, in-depth discussions between the supervisors and the Issuer of Prepaid Payment Instruments to implement remediation measures shall follow. If, however, a serious problem has already arisen or high urgency in any other form is observed, the supervisors may go further and pinpoint the issues which the supervisors consider necessary to be rectified and then check the policies of each Issuer of Prepaid Payment Instruments for rectification.

(B) If an Issuer of Prepaid Payment Instruments is determined to be unlikely to cause the abovementioned serious problems, the Issuer is expected to exercise diverse initiatives to innovate itself in ways fitting its circumstances and to continue efforts to refine business models and risk management practices. The supervisory authorities shall try to deepen the understanding of the business conditions and challenges of Issuers of Prepaid Payment Instruments and their policies and strategies through day-to-day monitoring and profiling activities. Then, the supervisory authorities shall conduct in-depth dialogue with Issuers of Prepaid Payment Instruments to discuss their business models, risk management practices, human resources development, and other issues, without a presumption on specific answers, for the purpose of promoting their improved awareness and understanding (and share model cases of other Issuers of Prepaid Payment Instruments for best practices where appropriate).

(4) Response to inquiries, complaints, etc.

(i) Basic response

The Counseling Office for Financial Services Users of the FSA and the relevant division in charge at each Local Finance Bureau shall be the primary contact for receiving consultation and/or complaints, etc. concerning Issuers of Prepaid Payment Instruments and Prepaid Payment Instruments. These authorities shall explain to those who made such consultation and complaint etc. that they are not in a position to conduct mediation, etc. concerning individual transactions and, if necessary, introduce a Certified Association for Payment Service Providers to them as an institution to respond to such consultation, complaints, etc. pursuant to the law. If the person who made consultation or complaint, etc. has given consent to the provision of his/her information to the relevant Issuer of Prepaid Payment Instruments, the Local Finance Bureau having jurisdiction over such Issuer of Prepaid Payment Instruments shall, in principle, provide the information to the Issuer of Prepaid Payment Instruments.

(ii) Accumulation of information

Each Local Finance Bureau shall record (in Appended Form 1-2) the content of any consultations, complaints, etc. concerning Issuers of Prepaid Payment Instruments that are deemed to be helpful for ensuring the soundness of the business of Issuers of Prepaid Payment Instruments and, if the information is deemed particularly influential, it shall promptly report it to the relevant division in charge at the FSA.

(iii) Cooperation with the Counseling Office for Financial Services Users

To properly reflect feedback from consultation or complaints, etc. received at the Counseling Office for Financial Services Users, the supervisory departments shall take the

following measures.

(A) Analysis of details of the consultation and complaints, etc. circulated from the Counseling Office

(B) Exchange of information with the Counseling Office

(5) Grasp of the situations of business operators without notification or registration

If the supervisors become aware of any person who is engaged in the business of issuing Prepaid Payment Instruments for Own Business and who has not submitted a notification of issuance despite the amount of its Unused Base Date Balance exceeding the amount prescribed in Article 6 of the Order (hereinafter simply referred to as "without notification") or who is engaged in the business of issuing Prepaid Payment Instruments for Third-Party Business without registration (hereinafter collectively referred to as "unregistered business operator or the like") based on complaints from users, inquiries from the investigative authorities, information provided by an Issuer of Prepaid Payment Instruments or a Certified Association for Payment Service Providers, or advertisements in newspapers, etc., the supervisors shall actively endeavor to ascertain the actual status of said person by making inquiries to the police or local consumer affairs centers, etc. or by direct telephone confirmation, etc.

In particular, when there are complaints, etc. from users or inquiries from the investigative authorities, the supervisors shall not merely respond to them but pay sufficient attention to them.

(6) Handling of unregistered business operators or the like

When having received information concerning unregistered business operators or the like the supervisors shall endeavor to take the following measures to prevent the spread of damage.

(i) Receipt of complaints, etc.

Upon receiving information on an unregistered business operator or the like from users, etc., the supervisors shall hear the content of such information (its name, address, name of representative, telephone number, actual conditions of business, name of the applicant, and whether to notify the investigative authorities, etc. of the content of application), and then take the following measures.

(A) When receiving information on an unregistered business operator or the like whose principle place of business is located in the jurisdiction of another Local Finance Bureau, the Local Finance Bureau shall hear the content of information and then notify the Local Finance Bureau having jurisdiction over such business operator (in principle, the latter who is so notified will handle the case).

(B) With regards to a business operator whose contact information is unknown, the supervisors shall endeavor to seek further information.

(C) When requested by an informant not to contact the business operator or other organizations, the supervisors shall take care not to put the informant at a disadvantage.

(D) If the case involves a business operator suspected to be non-notification or unregistered, the supervisors shall suggest that the informant contact and give information to investigative authorities as well.

(E) The supervisors shall prepare "Management ledger (Appended Form 2)" and organize and record the content of complaints and inquiries relating to Issuers of Prepaid Payment Instruments and guidance of supervisory authorities to them, and their responses, etc. in chronological order

(ii) Cases where it is found that a business operator is conducting the business of issuing Prepaid Payment Instruments without notification or registration

If the name and contact information of a business operator is known from the information received directly or information provided by the FSA or other authorities, and its actual business situations are also known to some extent, the supervisors shall endeavor to ascertain the actual situations of the business operator by calling it directly or by other means. If, as a result, it is found that the business operator is engaged in the business of issuing Prepaid Payment Instruments without necessary notification or registration, the following measures shall be taken (except in cases where doing so may hinder the investigation by the investigative authorities).

(A) If the business operator fails to carry out necessary notification or registration due to lack of intent or malicious intent and is deemed not to have problems from the viewpoint of user protection, the supervisors shall immediately request the business operator to stop the business of issuing Prepaid Payment Instruments and require the Issuer of Prepaid Payment Instruments to register as the Issuer of Prepaid Payment Instruments for Own Business or the Issuer of Prepaid Payment Instruments for Third-Party Business.

(B) If the business operator fails to carry out necessary notification or registration willingly or with malicious intent and is deemed to have problems from the viewpoint of user protection, the supervisors shall notify a relevant investigative authorities to that effect and give a written warning in Appended Form 3 to immediately stop such act.

(iii) Cases where it cannot be concluded that the business operator is engaged in the business without notification or registration

If, as a result of the assessment of the actual situation, it cannot be concluded that the business operator is engaged in the business of issuing Prepaid Payment Instruments without notification or registration, but it is judged that there is a possibility that the business operator is engaged in the business, the supervisors shall make an inquiry in writing in accordance with Appended Form 4 (except in cases where doing so may hinder the investigation by the investigative authorities).

(iv) Cases where the business operator does not make correction despite the warning

If the business operator does not make correction despite the warning in the Appended Form 3, the supervisors shall file an accusation with the investigative authorities as necessary.

(v) Reporting to the FSA

In cases where supervisors have taken a measure such as “warning” or “accusation,” the supervisors shall promptly send copies of the “Management ledger” and “Written warning” etc. to the Commissioner of the Financial Services Agency.

III-1-3 Coordination among Supervisory Authorities

(1) Cooperation between the FSA and Local Finance Bureaus

The Financial Services Agency and Local Finance Bureaus need to share awareness of issues deemed necessary for the supervision of Issuers of Prepaid Payment Instruments by appropriately exchanging relevant information. For this reason, the FSA and the Local Finance Bureaus shall make efforts to strengthen the mutual cooperation, such as by providing information in timely and appropriate manner and actively exchanging opinions, etc., with regard to information, etc. other than the coordination, etc. pertaining to internal delegated affairs listed in III-1-5, as well. In addition, the Local Finance Bureaus shall endeavor to strengthen cooperation between themselves by, when they become aware of any undisclosed

issues regarding an Issuer of Prepaid Payment Instruments supervised by another Local Finance Bureau, providing information to the relevant Local Finance Bureaus or the FSA as appropriate.

III-1-4 Cooperation, etc. with Certified Association for Payment Service Providers

Certified Associations for Payment Service Providers (hereinafter collectively referred to as "the Association") have an important role to play in ensuring the proper operation of the business of Issuers of Prepaid Payment Instruments, thereby promoting the sound development of Prepaid Payment Instruments and protection of the interests of users, and contributing to the improvement of the safety, efficiency, and convenience of the payment system, including the establishment of self-regulatory rules, the investigation and guidance of the status of legal compliance, etc. to members, and the resolution of complaints from users.

In supervising Issuers of Prepaid Payment Instruments, it is necessary to ensure appropriate cooperation not only among the Local Finance Bureaus and the divisions in charge of the Financial Services Agency but also among the three parties including the Association. For the three-party cooperation, each of them should pay attention to the following.

(1) From the viewpoint of conducting efficient and effective supervision of Issuers of Prepaid Payment Instruments who are members of the Association, the supervisors shall hold an interview as needed with regard to the investigations, audits, guidance for improvement, etc. conducted by the Association for its members.

(2) For minor matters that are not necessarily in violation of laws and regulations and for which it is deemed appropriate and effective for the Association to provide improvement guidance, etc., the supervisors may, in close cooperation with the Association, request the Association to give improvement guidance, etc. and to pay attention to such matters in its investigation, while taking into consideration the supervisory right of the authorities.

(3) With regard to complaints, etc. received by the Association and the status of processing complaints and the trend of the complaints, the supervisors shall hold an interview and exchange opinions with the Association.

(4) From the perspective of supervising Issuers of Prepaid Payment Instruments including non-members appropriately and efficiently, the supervisory authorities shall closely cooperate with the Association with regard to the establishment, amendment, and status of operation of the self-regulatory rules.

III-1-5 Internal Delegation

(1) Coordination with the Commissioner of the Financial Services Agency

The Director-General of a Local Finance Bureau shall, in processing the matters to be delegated to him/her regarding supervisory affairs of Issuers of Prepaid Payment Instruments, coordinate in advance with the Commissioner of the FSA with regard to the following matters (which does not preclude coordination with the Commissioner of the FSA with regard to other matters on an as-needed basis). It should be noted that, at the time of coordination, the Director-General of a Local Finance Bureau shall report the results of the deliberations made by his/her bureau (including deliberations made pursuant to III-3(3) hereof) and express the opinions thereof.

(i) Order to improve business operations under Article 25 of the Act

(ii) Suspension of business under Article 26 of the Act

(iii) Revocation of registration or business suspension under Article 27(1) of the Act

(2) Sub-delegation to the Head of Local Finance Office, etc.

In cases where the location of the principal business office or office of an applicant for notification of issuance of Prepaid Payment Instruments for Own Business, an applicant for registration of issuance of Prepaid Payment Instruments for Third-Party Business, and an Issuer of Prepaid Payment Instruments (hereinafter referred to as "business office, etc.") is within the jurisdictional district of a Local Finance Office, the Otaru Sub-office of Hokkaido Local Finance Bureau, or the Kitami Sub-office of Hokkaido Local Finance Bureau, the authorities delegated to the Director-General of a Local Finance Bureau pertaining to the acceptance of written notification, applications and reports submitted by the applicant for notification, the applicant for registration, or the Issuer of Prepaid Payment Instruments may be delegated to the Head of said Local Finance Office or Sub-Office.

The written notifications, etc. concerning these matters shall be submitted to the attention of the Director-General of the Local Finance Bureau having jurisdiction over the location of the principal business office, etc. of an applicant for notification, an applicant for registration, or an Issuer of Prepaid Payment Instruments.

Exhibit 1: Basic Procedures for On-Site Inspection
Exhibit 1-2: List of Important Matters

III-2 Various Administrative Procedures concerning the Payment Services Act

Administrative processes pertaining to the notification of issuance of Prepaid Payment Instruments for Own Business, the application for and change of the registration of Issuer of Prepaid Payment Instruments for Third-Party Business, and the inspection of the register of Issuer of Prepaid Payment Instruments for Own Business and the register of Issuer of Prepaid Payment Instruments for Third-Party Business (hereinafter referred to as "register, etc.") shall be handled as follows.

III-2-1 Acceptance, etc. of Notification of Issuance and Application for Registration

(1) Acceptance of notification of issuance of Prepaid Payment Instruments for Own Business

(i) When accepting a notification of issuance and/or notification of change thereof, the supervisors shall pay attention to the following matters and, if finding them inappropriate, request the Issuer of Prepaid Payment Instrument who submitted the notification to make a correction.

(A) The applicant must not use any trade name or name that is likely to mislead users of Prepaid Payment Instruments to think as if it is a public institution or a well-known organization or it has a special relationship therewith, or to impair the fairness of transactions.

(B) The applicant must not make two or more applications for notification using two or more trade names or names.

(C) The entrustment agreement with entrustees must cover the following matters.

a) The entrustees' obligation to comply with the Payment Services Act
b) Matters concerning the scope of entrusted operations
c) Matters concerning how to determine and how to pay the commission to entrustees
d) Sharing of expenses necessary for handling the entrusted operations;
e) Entities to install business facilities and equipment

(ii) Business offices, etc.

(A) The term "the business office or office pertaining to the business of issuing Prepaid Payment Instruments" as used in Article 5(1)(iii) of the Act means a certain place where an Issuer of Prepaid Payment Instruments for Own Business repeatedly and continuously is engaged in the business of issuing Prepaid Payment Instruments for Own Business in whole or in part.

(B) The term "the location where the major business activities for issuing Prepaid Payment Instruments are conducted;" prescribed in Note 1 on page 3 of Appended Form 1 of the Cabinet Office Order means the principal business office, etc. of the Issuer and the business office, etc. at which Prepaid Payment Instruments are issued, and does not include unmanned charging stations.

(2) Processing, etc. of notification of change of Issuer of Prepaid Payment Instruments for Own Business, etc.

In cases where the change so notified is a change of the location of the principal business office, etc. beyond the jurisdictional district of the Local Finance Bureau, such change shall be treated as follows.

(A) The Director-General of the Local Finance Bureau who has received the relevant notification of change, etc. shall notify the Director-General of the Local Finance Bureau with jurisdiction over the location of the new principal business office, etc. thereof with the written notification of change prepared using Appended Form 5, together with a copy, etc. of the relevant Notification of Change, the written opinion of the Local Finance Bureau prepared using Appended Form 6, and the previous notification and documents to be attached thereto, as well as the report on the issuance as of the immediately preceding Base Date (Note) and the report on the inspection conducted immediately prior to the notification.

Note: In the case where the provision of Article 29-2(1) of the Act applies, a copy of the notification in the same paragraph shall be attached, and the report on issuance shall be attached not only to a case where it relates to the immediately preceding Base Date but also to the extent necessary for supervision.

(B) The Director-General of the Local Finance Bureau who received the written notice set forth in (A) above shall, without delay, prepare a register of Issuers of Prepaid Payment Instruments for Own Business, and notify the Director-General of the Local Finance Bureau who originally received the notification to that effect by a written notice of completion of preparation of the register prepared using Appended Form 7. When said notice has been given, the Director-General of the Local Finance Bureau who originally received the notification shall delete the registration of such Issuer of Prepaid Payment Instruments for Own Business from the register of Issuers of Prepaid Payment Instruments for Own Business and send the necessary documents to the Director-General of the Local Finance Bureau to which the registration is transferred.

(3) Acceptance of application for registration of Issuers of Prepaid Payment Instruments for Third-Party Business

(i) When accepting an application for registration and/or notification of change thereof, the supervisors shall pay attention to the following matters and, if finding them inappropriate,

request the Issuer of Prepaid Payment Instrument who submitted the application and/or notification to make a correction.

(A) The applicant must not use any trade name or name that is likely to mislead purchasers of Prepaid Payment Instruments to think as if it is a public institution or a well-known organization or it has a special relationship therewith, or to impair the fairness of transactions.

(B) The applicant must not make two or more applications for registration using two or more trade names or names.

(C) The entrustment agreement with entrustees must cover the following matters.

a) The entrustees' obligation to comply with the Payment Services Act

b) Matters concerning the scope of entrusted operations

c) Matters concerning how to determine and how to pay the commission to entrustees

d) Sharing of expenses necessary for handling the entrusted operations;

e) Entities to install business facilities and equipment

(ii) Business offices, etc.

(A) The term "the business office or office pertaining to the business of issuing Prepaid Payment Instruments" as used in Article 8(1)(iii) of the Act means a certain place where an Issuer of Prepaid Payment Instruments for Third-Party Business is repeatedly and continuously engaged in the business of issuing Prepaid Payment Instruments for Third-Party Business in whole or in part.

(B) The term "the location where the major business activities for issuing Prepaid Payment Instruments are conducted;" prescribed in Note 1 on page 3 of Appended Form 3 of the Cabinet Office Order means the principal business office, etc. of the Issuer and the business office, etc. at which Prepaid Payment Instruments are issued, and does not include unmanned charging stations.

(4) Examination of application for registration of Issuers of Prepaid Payment Instruments for Third-Party Business

(i) When examining the registration, the supervisors shall examine, in particular, the cases involving sophisticated and complex business models and systems in cooperation with the FSA as necessary.

(ii) The supervisors needs to keep in mind to conduct the examination efficiently.

Note:For example, the examiner should pay attention not to take a long time to verify the merely formal part of the registration or not to overlap the verification items of the Local Finance Office and the Local Finance Bureau.

(iii) The supervisors should be careful to make an integrated examination for an applicant who intends to apply for the registration of issuing the Prepaid Payment Instruments for Third-Party Business and for the Funds Transfer Service at the same time, for providing integrated services of both businesses.

(iv) The supervisors shall assess the financial foundation under Article 10(1)(ii) of the Act in accordance with the following.

(A) For a newly established organization, its financial foundation shall be assessed based on its balance sheet at the time of establishment.

(B) In cases falling under Article 5(1)(ii) of the Order, how to manage the amount of the unused balance of issued Prepaid Payment Instruments minus the balance of security deposit for issuance shall be checked in light of its internal rules.

(C) When confirming the content of the "the latest balance sheet (including the related notes) and profit and loss statement (including the related notes) or any substitute thereof" under item (vi) of Article 16 of the Cabinet Office Order in the case where the applicant does not hold the documents (audit certificate) under item (vii) of said Article, the following documents, for example, shall be used as necessary.

a) If savings are recorded, a certificate of the balance issued by a financial institution who trades with the applicant;

b) In cases where securities are recorded, a report on the balance of transactions issued by a securities company who trades with the applicant;

c) In cases where land or buildings are recorded, a copy of fixed asset valuation certificate issued by a municipality or appraisal report prepared by a real estate appraiser;

d) A copy of a tax return for corporation tax and a copy of the balance sheet attached thereto

(v) In conducting the examination under Article 10 (1)(iii) and (iv) of the Act, the supervisors shall pay attention to whether a control environment has been established to appropriately respond to the main viewpoints listed in II-3-3-1 in light of the scale and characteristics of issuance described in the applicant's written application for registration.

(vi) In examining whether an applicant falls under the category of a "corporation which has not established a system that is necessary for ensuring compliance with the provisions of this Chapter" as prescribed in Article 10(1)(v) of the Act, the supervisors shall hold thorough interviews and on-site inspections based on the written application for registration and the attached documents, and, in particular, pay attention to the following points.

(A) Has the applicant developed a control environment for appropriately responding to the main viewpoints listed in II-1 to II-3 hereof in light of the scale and characteristics of the issuing business described in the applicant's written application for registration?

(B) In particular, when confirming the organizational structure, has the applicant secured sufficient personnel commensurate with the structure of the Internal Control Department (or the Internal Audit Department depending on type of its business) in which the mutual check function effectively works, including the structure for legal compliance?

(5) Processing of application for registration of Issuers of Prepaid Payment Instruments for Third-Party Business

(i) A written notice of completion of registration under Article 17 of the Cabinet Office Order shall be treated as follows.

(A) In cases where an applicant Issuer of Prepaid Payment Instruments for Third-Party Business has submitted a written application for registration through a relevant Local Finance Office or sub-office pursuant to Article 54 of Cabinet Office Order, the written notice of completion of registration shall be delivered at such Local Finance Office or sub-office.

(B) The registration number shall be given serially from 00001 in the order of completion of approvals by the Directors-General of Local Finance Bureaus.

(C) When a registration is no longer valid, its registration number shall be retired and no replacement shall be made.

(D) With regard to a notification for change of the location of the principal business office, etc., which is beyond the jurisdictional district of the local finance bureau, its registration

number shall be newly given by the Director-General of the Local Finance Bureau who effected the new registration in serial in accordance with (B) above.

(ii) If a registration is refused, a written notice of refusal of registration, stating the reasons for refusal, etc., based on Article 19(3) of the Cabinet Office Order shall be delivered to the registration applicant (See III-4).

(iii) When refusing the registration, the Director-General of the Local Finance Bureau shall notify the Director-General of the Supervisory Bureau of the FSA to that effect by sending a written notice of refusal of registration of Issuer of Prepaid Payment Instruments for Third-Party Business using the Appended Form 8 together with a copy of written application for registration.

(6) Interview, etc. after registration

During the period from the registration to commencement of business, the supervisors shall conduct interviews and on-site inspections, etc. to confirm whether the applicant can start the business of issuing Prepaid Payment Instruments normally.

(7) Processing, etc. of notification of change of Issuer of Prepaid Payment Instruments for Third-Party Business

(i) If it becomes clear that a person newly appointed as an officer of the notifier falls under any of Article 10(1)(ix)(a) through (e) of the Act, the supervisory authorities shall take measures such as revocation of registration prescribed in Article 27 of the Act with respect to the notifier.

(ii) In cases where the change so notified is a change of the location of the principal business office, etc. beyond the jurisdictional district of the Local Finance Bureau, such change shall be treated as follows.

(A) The Director-General of the Local Finance Bureau who receives the notification of change of registered matters shall retain the attached documents under Article 20(1)(vii) of the Cabinet Office Order (the written notice of completion of registration).

(B) The Director-General of the Local Finance Bureau who has received the relevant notification of change, etc. under (A) above shall notify the Director-General of the Local Finance Bureau who will newly have the authority of registration pursuant to Article 20(2) of the Cabinet Office Order, with the written notification of change prepared using Appended Form 9, together with a copy of the relevant Notification of Change, the part of the register of Issuer of Prepaid Payment Instruments for Third-Party Business relating to the notifier, the written opinion of the Local Finance Bureau prepared using Appended Form 10, and the previous written application for registration and documents to be attached thereto, as well as a report on the issuance of the immediately preceding Base Date (Note) and the report on the inspection conducted immediately prior to the submission of the relevant Notification of Change.

Note: In the case where the provision of Article 29-2(1) of the Act applies, a copy of the notification in the same paragraph shall be attached, and the report on issuance shall be attached not only to a case where it relates to the immediately preceding Base Date but also to the extent necessary for supervision.

(C) The Director-General of a Local Finance Bureau who received the written notice set forth in (B) above shall, without delay, register it on the register of Issuers of Prepaid Payment Instruments for Third-Party Business, and notify the Director-General of a

Local Finance Bureau who originally received the notification to that effect by a written notice of completion of preparation of the register prepared using Appended Form 11. When said notice has been given, the Director-General of the Local Finance Bureau who originally received the notification shall delete the registration of such Issuer of Prepaid Payment Instruments for Third-Party from the register of Issuers of Prepaid Payment Instruments for Third-Party Business and send the necessary documents to the Director-General of the Local Finance Bureau who prepared a new registration.

(8) Issuance of certificates of registration

If a registered Issuer of Prepaid Payment Instruments for Third-Party Business or a person who was an Issuer of Prepaid Payment Instruments for Third-Party Business files an application for the registration certificate for the reason that it is necessary to submit it to a public institution, etc., the supervisors shall issue a certificate of registration for the Issuer of Prepaid Payment Instruments for Third-Party Business pursuant to Appended Form 12. Provided, however, that this shall not apply to cases where the registration application documents have already been disposed of after the expiration of the retention period.

(9) Preparation of a register of Issuers of Prepaid Payment Instruments for Own Business and a register of Issuers of Prepaid Payment Instruments for Third-Party Business

(i) Preparation of a register of Issuers of Prepaid Payment Instruments for Own Business

The supervisors shall prepare a list of Issuers of Prepaid Payment Instruments for Own Business who made the notification based on the Notification of Issuance under Article 9 of the Cabinet Office Order (pages 2 to 9 of Appended Form 1 of the Cabinet Office Order) by organizing each of the written notifications so submitted.

(ii) Preparation of a register of Issuers of Prepaid Payment Instruments for Third-Party Business

The supervisors shall prepare a register of Issuers of Prepaid Payment Instruments for Third-Party Business who made the notification based on the Application for Registration under Article 14 of the Cabinet Office Order (pages 2 to 9 of Appended Form 3 of the Cabinet Office Order) by organizing each of the written applications so submitted.

(10) Public inspection of the register of Issuers of Prepaid Payment Instruments for Own Business and the register of Issuers of Prepaid Payment Instruments for Third-Party Business

The public inspection of the register of Issuers of Prepaid Payment Instruments for Own Business pursuant to Article 13 of the Cabinet Office Order and the public inspection of the register of Issuers of Prepaid Payment Instruments for Third-Party Business pursuant to Article 18 of the Cabinet Office Order shall be conducted as follows.

(i) A person who made a request for public inspection shall be required to fill in the prescribed items on the application for public inspection of the register of Issuers of Prepaid Payment Instruments for Own Business or the register of Issuers of Prepaid Payment Instruments for Third-Party Business pursuant to Appended Form 13. It should be noted that a person who has changed his/her surname may also enter his/her former surname (meaning the former surname prescribed in Article 30-13 of the Order for Enforcement of the Residential Basic Book Act (Cabinet Order No. 292 of 1967, the same shall apply in III-2-5)) and name between parentheses in the column of "Applicant's name."

(ii) The date and time of inspection of the register shall be as follows.

(A) The date of public inspection shall be days other than Saturdays, Sundays, holidays

prescribed in Article 3 of the Act on National Holidays, January 2 and 3, and from December 29 to 31.

(B) The public inspection time shall be within the time specified by the Director-General of the Local Finance Bureau.

(C) When it is necessary to organize the register, etc. or for any other reason, the public inspection date or time may be changed.

(iii) The register, etc. may not take out of the place of the public inspection designated by the Director-General of the Local Finance Bureau.

(iv) The following persons may be suspended or refused for public inspection:

(A) Any person who fails to follow (1) through (3) above or the instructions of the staff;

(B) Any person who has damaged or is deemed likely to damage the register, etc.

(C) Any person who has caused or is deemed likely to cause trouble to others.

(11) Periodic reporting, etc. on issuance of Prepaid Payment Instruments

(i) Periodic reporting on issuance of Prepaid Payment Instruments

The Director-General of a Local Finance Bureau shall send to the Director-General of the Supervisory Bureau of the FSA a Survey Sheet on Notification/Registration Status in the form prescribed in Appended Form 14 and a Survey Sheet on Outstanding Balance of Prepaid Payment Instruments in the form prescribed in Appended Form 15, by the end of three months from the month following each ordinary Base Date.

(ii) Submission of a list of the notifications of Issuers of Prepaid Payment Instruments for Own Business and the registrations of Issuers of Prepaid Payment Instrument for Third-Party Business

(A) Local Finance Bureau (or relevant Local Finance Office or Sub-office) shall update a list of notification and registration status for all notified Issuers of Prepaid Payment Instruments for Own Business and all registered Issuers of Prepaid Payment Instruments for Third-Party Business in the form prescribed in Appended Form 16 each time a notification or registration is filed, and send a copy of said list to the Director-General of the Supervisory Bureau of the FSA within twenty (20) days after each Base Date.

(B) The list must always include the following;

- Name of Issuer
- Address of Issuer
- Phone number of Issuer
- Description of goods or services received through use of Prepaid Payment Instruments
- Whether the Prepaid Payment Instruments show the amounts or the quantity

III-2-2 Handling of Discontinuation of Business of Issuing Prepaid Payment Instruments

(1) If an Issuer of Prepaid Payment Instruments has decided to discontinue all or part of the business of issuing Prepaid Payment Instruments (excluding the cases where such discontinuance resulted from inheritance, transfer of business, merger or company split, or for other reasons) pursuant to Article 24(1) of the Act, or has become subject to revocation of the registration as an Issuer of Prepaid Payment Instruments for Third-Party Business pursuant to Article 27(1) of the Act, the Director-General of a relevant Local Finance Bureau shall request the Issuer of Prepaid Payment Instruments to submit a written report in the form of Appended Form 17 stating the schedule for implementation of the procedure for refund of Prepaid Payment Instruments under Article 20(1) of the Act.

Note 1: It should be kept in mind that if a notification of discontinuance, etc. of part of the business of issuing Prepaid Payment Instruments is submitted pursuant to Article 33(1) of the Act, only the Prepaid Payment Instruments pertaining to said discontinued business will be subject to the refund procedure prescribed in Article 20(1) of the Act.

Note 2: The cases "when the Issuer of Prepaid Payment Instruments has discontinued all or part of the business of issuing Prepaid Payment Instruments" prescribed in Article 33(1)(i) of the Act refers to cancellation of both issuance and use of said Prepaid Payment Instruments and does not include cancellation of only new issuance.

(2) In cases where a written notification of discontinuance, etc. of Prepaid Payment Instruments has been submitted by an Issuer of Prepaid Payment Instruments pursuant to Article 33(1)(i) of the Act (limited to cases where said business was succeeded to an Issuer of Prepaid Payment Instruments for Own Business (including those deemed to be an Issuer of Prepaid Payment Instrument for Own Business under Article 30(1) of the Act) or to a registered Issuer of Prepaid Payment Instruments for Third-Party Business who made a notification to the Director-General of another Local Finance Bureau, through inheritance, transfer of business, merger or company split, or for other reasons), the Director-General of the Local Finance Bureau who has received said written notification of discontinuance, etc. shall send the Notice of Business Transfer prepared by using Appended Form 18 together with a copy of said notification of discontinuance, and the portion of the register of Issuers of Prepaid Payment Instruments for Own Business or the register of Issuers of Prepaid Payment Instruments for Third-Party Business pertaining to said notifier and the report on the issuance of Prepaid Payment Instruments for the immediately preceding Base Date (Note) to the Director-General of a Local Finance Bureau who has accepted or registered the notification of Issuer of Prepaid Payment Instruments to which said business is transferred.

Note: In the case where the provision of Article 29-2(1) of the Act applies, a copy of the notification in the same paragraph shall be attached, and the report on issuance shall be attached not only to a case where it relates to the immediately preceding Base Date but also to the extent necessary for supervision.

(3) The Director-General of the Local Finance Bureau to which the written notice described in (2) above has been sent shall, without delay, confirm whether necessary measures, including the submission of a written notification of change pertaining to the business, have been taken with regard to the Issuer of the Prepaid Payment Instruments to which the relevant business has been transferred.

(4) When a report has been submitted pursuant to Article30(2) of the Act by an entity deemed to be an Issuer of Prepaid Payment Instruments for Own Business pursuant to Article 30(1) of the Act (hereinafter referred to as "successor"), the supervisors shall confirm whether a control environment has been established so that the successor can appropriately carry out the business of issuing Prepaid Payment Instruments, such as whether the means of providing goods and services and the security deposit for issuance pertaining to the Prepaid Payment Instruments subject to the succession have been succeeded to the successor.

III-2-3 Procedures for Security Deposit for Issuance

(1) Matters concerning a written notification of making, etc. of security deposit for issuance

(i) Replacement of security deposit for issuance

Approval for replacement of a security deposit for issuance pursuant to Article 4 of the Ordinance on Security Deposit for Issuance of Prepaid Payment Instruments (Ordinance of the Cabinet Office and the Ministry of Justice No. 4 of 2010) may be granted if a security deposit for issuance in lieu of the bond certificates prescribed in Article 14(3) of the Act has been deposited in advance.

(2) Matters concerning the recovery of security deposit for issuance

(i) "the Base Date immediately preceding the day on which such fact occurred" as prescribed in Article 9(1)(i) and (ii) of the Order shall mean the Base Date immediately preceding the date of submission of the application for approval of recovery of security deposit for issuance pursuant to Article 1(1) of the Ordinance on Security Deposit for Issuance of Prepaid Payment Instruments.

III-2-4 Handling of Base Date Report

(1) The following points shall be taken into consideration when processing a report on the issuance of Prepaid Payment Instruments prescribed in Appended Form 27 of the Cabinet Office Order (hereinafter referred to as the "Base Date Report").

(i) In the "Outline of issuance, etc." column, if Unused Base Date Balance is rapidly increasing or decreasing in comparison with the previous Unused Base Date Balance (Note), the supervisors shall seek causes of such increase or decrease by having interviews, etc., as necessary.

Note: In the case to which Article 29-2(1) of the Act applies, if the Record Period containing the date of submission of the notification set forth in the same paragraph is from the day following the special Base Date to the next ordinary Base date, the "previous Unused Base Date Balance" shall be the Unused Base Date Balance as of the ordinary Base Date immediately preceding said special Base Date.

(ii) Upon reviewing the financial statements attached to said Base Date Report and finding that there has been a significant change in the business condition of the Issuer of Prepaid Payment Instruments such as the recording of a current net loss or excessive liabilities, the supervisors shall confirm the forecast on its business condition and future plans pertaining to the business of issuing Prepaid Payment Instruments by having interviews, etc. as necessary.

(2) Sending to the FSA

If there is an Issuer of Prepaid Payment Instruments to whom the supervisors shall attach opinions with regard to (1)(i) and (ii) above, the supervisors shall prepare a written opinion and

promptly send it, together with a copy of the Base Date Report submitted by said Issuer of Prepaid Payment Instruments and the reference documents, to the relevant department in charge at the FSA.

III-2-5 Points of Attention regarding Statements in Reports Submitted by Issuers of Prepaid Payment Instruments

With regard to a name to be entered in Appended Forms, it should be noted that, in accordance with the procedures under the laws and regulations, a person who has submitted a notification of issuance, an application for registration or a notification of change by entering his/her former surname and name together may fill in their former surname and name together in parentheses or fill in their former surname and name instead of their current name.

III-2-6 Points of Attention regarding Written and Face-to-Face Procedures

An application and notification to be submitted by an Issuer of Prepaid Payment Instruments, etc. to competent authorities and a disposition notice, etc. to be issued by the competent authorities to an Issuer of Prepaid Payment Instruments, etc. may be made by using an electronic data processing system pursuant to Article 6(1) and Article 7(1) of the Act on Promotion of Administration by Use of Information and Communications Technology (hereinafter referred to as “Digital Procedure Act”) even if any other laws and regulations stipulate that such application, notification, etc. and disposition notice, etc. shall be made in writing, etc. or by other methods.

In light of the purpose of the Digital Procedures Act, the provisions of these Guidelines related to procedures covered by the Digital Procedures Act may also be fulfilled by means of an electronic data processing system, regardless of the provisions requiring a written or face-to-face means.

In addition, while digitization is rapidly advancing in all economic and social activities, the Government as a whole is reviewing Japan's systems and practices based on written, stamped, and face-to-face procedures, and is moving forward with efforts toward the realization of a remote society in which procedures can be carried out without actually having to travel.

In order to steadily advance these efforts, the FSA has also promoted the computerization of administrative procedures by updating the FSA Electronic Application and Notification System, which enables online submission of all procedures for applications and notifications received from Issuers of Prepaid Payment Instruments, etc., and by revising Cabinet Office Orders and supervisory guidelines to abolish seals.

Furthermore, with regard to procedures between private business operators, as well, the FSA established the “Panel for Reviewing Procedures Requiring Documents, Seals, and Face-to-Face Contact in the Financial Industry” to encourage the industry as a whole to review conventional practice and has made efforts to promote digitalization of documents, to eliminate the seal procedures and to review face-to-face requirements.

In light of such efforts by the public and private sectors, written and/or face-to-face requirements in these Guidelines other than those related to procedures covered by the Digital Procedure Act may also be fulfilled by means of an electronic data processing system or other information and communications technology, except for cases where the submission of an original document is required in III-2-7 hereof.

Considering the intent of the abovementioned handling, the FSA and relevant supervisory authorities shall promote conduct of procedures based on the provisions of these Guidelines in a manner other than in writing or in person, whenever possible, taking into account the intentions of the parties to the procedures.

III-2-7 Points of Attention when Submitting Applications, etc.

Based on III-2-6 hereof, the FSA and relevant supervisory authorities shall require, in principle, that applications and/or notifications by Issuers of Prepaid Payment Instruments, etc. be submitted by the deadline specified by relevant laws and regulations using the FSA Electronic Application and Notification System.

Provided, however, that with regard to an attached document issued by a public institution (a copy of certificate of residence, warrant card, a copy of family register, documents certifying payment of taxes, fees, etc.) and an attachment document concerning procedures for a petition for the execution of the right pertaining to a security deposit for issuance and procedures for the filing of a claim pertaining to Prepaid Payment Instruments, the original thereof is required to be sent.

For the time being, e-Gov on the website of the FSA is also available for submission of notifications, applications, or other procedures that are allowed to be processed through e-Gov, in parallel with the FSA Electronic Application and Notification System.

III-3 Points of Attention in Enforcing Administrative Dispositions

Major adverse dispositions (as defined in Article 2(iv) of the Administrative Procedure Act; the same applies hereinafter) enforced by the supervisory authorities include: (i) the issuance of an order to improve business operations under Article 25 of the Act, (ii) the issuance of an order to suspend business under Article 26 or Article 27 of the Act, and (iii) the revocation of a registration under Article 27 of the Act. The basic workflow for rendering such administrative dispositions is illustrated as follows.

(1) Order to submit reports pursuant to Article 24 of the Act

(i) If the on-site inspection or off-site monitoring (such as interviews) finds out any problem in compliance management systems, governance systems, or other business practices of the inspected Issuer of Prepaid Payment Instruments, the supervisors shall ask it to report its fact-checking of the problems, its own analyses of the causes of those problems, planned measures for improvement or remediation, and other necessary matters pursuant to Article 24(1) of the Act.

(ii) If the supervisors determine, as a result of verifying the report submitted by the Issuer of Prepaid Payment Instruments, that further scrutiny is needed, the supervisors shall ask it to submit an additional report pursuant to Article 24(1) of the Act.

(2) Follow-up on measures for improvement or remediation reported under Article 24(1) of the Act

(i) If the supervisors determine, as a result of verifying the reports submitted by an Issuer of Prepaid Payment Instruments, that no serious issue is found in terms of the soundness and appropriateness of its business and that the Issuer of Prepaid Payment Instruments is capable of promoting its self-initiated improvement efforts, the supervisors shall follow up on the progress of its measures for improvement reported in (1) above through non-compulsory interviews or other communication.

(ii) If necessary, the supervisors may ask the Issuer of Prepaid Payment Instruments to submit periodic follow-up reports pursuant to Article 24(1) of the Act.

(3) Order to improve business operations, order to suspend business, or revocation of registration based on Article 25, Article 26, or Article 27 of the Act

In cases where, as a result of examining the contents of the report (including additional reports)

as a response to inspection results and offsite monitoring, it is found that there are serious problems with ensuring the sound and appropriate management of the business of issuing Prepaid Payment Instruments, including the protection of the interests of users, etc., the supervisors shall take into consideration the factors listed in (1) through (3) below:

- Whether it is appropriate to leave initiatives for improvement to voluntary efforts of the Issuer of Prepaid Payment Instruments;
- Whether it needs considerable efforts for the improvement and whether the Issuer of Prepaid Payment Instruments needs to focus on the business improvement for a certain period of time; and
- Whether it is appropriate for the Issuer of Prepaid Payment Instruments to continue the business;

and examine whether there are any other factors to be considered and determine the content of the final administrative disposition.

(i) Severity and maliciousness of the misconduct

(A) Degree of detriment to public interests

Does the Issuer of Prepaid Payment Instruments seriously harm the public interest by severely impairing the credibility of Prepaid Payment Instruments?

(B) Degree of damage to users

Do a large number of users in extensive areas suffer damage? How serious is each user's damage?

(C) Maliciousness of the improper conduct

Did the Issuer of Prepaid Payment Instruments commit a malicious act by, for example, making a false report on Unused Base Date Balance in order to avoid making a security deposit for issuance?

(D) Duration of the improper conduct and its repetitions

Has the conduct in question been continued over a long time or for a short period? Was it committed repeatedly or continuously? Or only once? Had the Issuer of Prepaid Payment Instruments committed any similar violation in the past?

(E) Intentionality

Did the Issuer of Prepaid Payment Instruments intentionally commit such act with an awareness of illegality or inappropriateness? Or was it mere negligence?

(F) Institutional involvement

Was the conduct in question at the sole discretion of a person in charge or based on directions from a high-level officer? Were the management team of the Issuer of Prepaid Payment Instruments involved in the conduct?

(G) Attempt to cover up the improper conduct

After the Issuer of Prepaid Payment Instruments or the persons in charge had recognized the problem, did they attempt to conceal its evidence? If so, was it an institutional attempt?

(H) Involvement of anti-social forces

Were any anti-social forces involved in the conduct in question? If so, to what extent were they involved?

(ii) Appropriateness of governance systems and business operation systems leading to the causes of the improper conduct

(A) Is the management team of the Issuer of Prepaid Payment Instruments fully aware of the significance of compliance and eager to promote compliance-conscious management?

(B) Is the Internal Audit Department of the Issuer of Prepaid Payment Instruments well prepared? Does it exert its functions properly?

(C) Are relevant staff of the Issuer of Prepaid Payment Instruments fully aware of the significance of compliance? Are they adequately trained or educated?

(iii) Mitigating factors

In addition to (i) and (ii) above, are there any factors that can allow the regulator to mitigate administrative enforcement? For example, is the Issuer of Prepaid Payment Instruments promoting self-initiated efforts for protecting users, etc. of Prepaid Payment Instruments before receiving any administrative measure?

(4) Standard period for processing a case subject to administrative disposition

Supervisory dispositions pursuant to Articles 25, 26, and 27(1) of the Act, if any, shall be given within approximately one (1) month (or approximately two (2) months if coordination with the FSA is required), in principle, from the time of receipt of the report described in (1) above.

Note 1: The following points should be taken into consideration in determining "the time of receipt of the report".

(A) If asking for submission of a report multiple times pursuant to Article 24(1) of the Act (limited to the case where each request for submission is made within the time frame specified above after receiving the immediately preceding report), the time for receiving the last report is regarded as the starting point of the time frame for administrative disposition.

(B) If asking for correction of a document submitted or for submission of additional documents (excluding inconsequential correction or provision of trivial information), such correction of the document or submission of additional documents is regarded as the starting point of the time frame for administrative disposition.

Note 2: The time spent for formal explanations or hearings is not included in the standard period for processing a case subject to administrative disposition.

Note 3: The standard period for processing a case subject to administrative disposition will apply to each set of information to be examined as the basis for invoking administrative disposition.

(5) Cancellation of the obligation to make progress reports based on the order to improve business operations issued under Article 25 of the Act

After issuance of an order to improve business operations to an Issuer of Prepaid Payment Instruments under Article 25 of the Act, the supervisors shall, in principle, ask the Issuer of Prepaid Payment Instruments to report the progress of its business improvement plan so that the supervisors can follow up on the approach of the Issuer of Prepaid Payment Instruments for business improvement based on such order and encourage its improvement efforts. For this, the following points shall be taken into consideration.

(i) If the supervisors ask an Issuer of Prepaid Payment Instruments to which it has issued an order to improve business operations pursuant to Article 25 of the Act to submit a report on the progress of the business improvement plan within a limited period, the Issuer of Prepaid Payment Instruments shall be relieved of the obligation to submit a report after expiration of the specified period.

(ii) If the supervisors ask an Issuer of Prepaid Payment Instruments to which it has issued an order to improve business operations pursuant to Article 25 of the Act to submit a report on

the progress of the business improvement plan on an ongoing basis without specifying a definite period, the supervisors shall cancel the obligation of the Issuer of Prepaid Payment Instruments to submit a report when the supervisors determine that adequate improvement measures have been completed in line with the business improvement plan to address the problem triggering the order to improve business operations. In this regard, the supervisors determine whether or not to cancel the obligation of the Issuer of Prepaid Payment Instruments to submit a report by evaluating its improvement efforts reported by the Issuer of Prepaid Payment Instruments or confirmed through the supervisor's inspections.

III-4 Relationship with the Administrative Procedure Act and Other Relevant Acts

(1) Relationship with the Administrative Procedure Act

When the supervisors intend to render any adverse disposition falling under any of the cases set forth in Article 13(1)(i) of the Administrative Procedure Act to an Issuer of Prepaid Payment Instruments, the supervisors must conduct hearings with the Issuer of Prepaid Payment Instruments. In case of any adverse disposition falling under the case set forth in item (ii) of the same article, the supervisors must offer the opportunity for explanation to the Issuer of Prepaid Payment Instruments.

In either case, the supervisors must show the grounds for the adverse disposition pursuant to Article 14 of the same act. (When such adverse disposition is rendered in writing, its grounds must also be indicated in writing.)

If intending to refuse to grant the permission, license, or other approval requested under an application filed by an Issuer of Prepaid Payment Instruments, the supervisors must show the grounds for the disposition of refusal pursuant to Article 8 of the same act. (When such disposition is rendered in writing, its grounds must also be indicated in writing.)

On this occasion, merely enumerating the provisions of relevant acts is not sufficient; instead, full accountability is required to clarify what facts underlie the decision to render the disposition and which acts and standards are relied on to justify the disposition.

(2) Relationship with the Administrative Complaint Review Act

If the supervisors intend to render any disposition against which a complaint may be filed, it should be kept in mind that the supervisors must explain in writing that the Issuer of Prepaid Payment Instruments is entitled to file a complaint pursuant to Article 82 of the Administrative Complaint Review Act (Act No. 68 of 2014).

(3) Relationship with the Administrative Case Litigation Act

If the supervisors intend to render any disposition against which an action for revocation may be filed, it should be kept in mind that the supervisors must explain in writing that the Issuer of Prepaid Payment Instruments is entitled to file a lawsuit pursuant to Article 46 of the Administrative Case Litigation Act (Act No. 139 of 1962).

III-5 System for Exchange of Opinions

Before rendering any adverse disposition to an Issuer of Prepaid Payment Instruments, the supervisors are supposed to conduct hearings with the Issuer of Prepaid Payment Instruments or give an opportunity for explanations to the Issuer of Prepaid Payment Instruments in accordance with the Administrative Procedure Act. In addition to and apart from such hearings or explanations, there is a system to allow the Issuer of Prepaid Payment Instruments to ask for multi-level exchange

of opinions between the supervisory authorities and the Issuer of Prepaid Payment Instruments. This system is meaningful to help the parties share the same recognition as to the facts underlying the disposition and their severity.

In cases where, in the course of interviews, etc. in relation to the supervisory authorities' request for reporting under Article 24(1) of the Act, an Issuer of Prepaid Payment Instruments who was aware that an adverse disposition is likely to be rendered requested the supervisory authorities to have an opportunity of exchange of opinions between the supervisory authorities' senior officials and the executives of the Issuer of Prepaid Payment Instruments (Note) and when the supervisory authorities intends to render an adverse disposition which requires prior hearings or the grant of an opportunity for explanations, the supervisory authorities must provide an opportunity for exchanging opinions as to the facts underlying the intended adverse disposition and their severity. Such opinion exchange session must be held before giving a notice of hearings or notice of granting an opportunity for explanations except where such disposition needs to be urgently rendered.

Note: Requests by an Issuer of Prepaid Payment Instruments for an opportunity for exchange of opinions must be made during the period from the time when the supervisory authorities received a written report under Article 24(1) 1 of the Act explaining the facts underlying the intended adverse disposition to the time when the supervisory authorities give a notice of hearing or of granting an opportunity for explanation.

III-6 Ascertainment of Locations of Business Office, etc.

Where it is necessary to ascertain the location of the business office, etc. of a registered Issuer of Prepaid Payment Instrument for Third-Party Business pursuant to Article 27(2) of the Act, the supervisors may require said Issuer of Prepaid Payment Instruments for Third-Party Business to submit a location report pertaining to the business office prepared using Appended Form 19, a document certifying the rights to the business office, etc., a map of the business office, etc., or a report such as a map of the business office, etc. pursuant to Article 24(1) of the Act. The supervisors may order that such report be submitted to the Local Finance Bureau having jurisdiction over the location of such business office, etc.

III-7 Basic Stance for Public Disclosure of Adverse Dispositions

(1) When making public notice of adverse disposition pursuant to Article 29 of the Act, the supervisory authorities shall disclose the following particulars in the public notice.
   (i) Trade name or name
   (ii) Name of the representative
   (iii) Location of the principal business office, etc.
   (iv) Registration number (for Issuer of Prepaid Payment Instruments for Third-Party Business only)
   (v) Date of registration (or date of notification for Issuer of Prepaid Payment Instruments for Own Business)
   (vi) Date of the disposition
   (vii) Details of the disposition

(2) It should be noted that the handling of public notice other than (1) above is based on the approach specified in "I-5 Transparency" of the "Principles of Financial Supervision and Instructions for Supervisory Department Staff (Code of Conduct)".

That is, with regard to the adverse dispositions such as orders to improve business operations,

etc., the facts underlying the invocation of those dispositions, the content of dispositions, and other information shall be made public from the viewpoint of enhancing predictability for other Issuers of Prepaid Payment Instruments and preventing recurrence of similar incidents or problems, except where the disclosure of relevant facts and information is likely to impede the business improvement efforts of the Issuer of Prepaid Payment Instruments concerned.

III-8 Notification of Administrative Disposition

(1) In the case of a refusal of registration (Article 10 of the Act)

When refusing the registration, the Director-General of the Local Finance Bureau shall notify the Director-General of the Supervisory Bureau of the FSA to that effect by sending a written notification of refusal of registration of Issuer of Prepaid Payment Instruments for Third-Party Business using the Appended Form 8 together with a copy of the written application for registration.

(2) In the case of an order to improve business operations (Article 25 of the Act)

When issuing an order to improve business operations, the Director-General of the Local Finance Bureau shall send relevant materials to the department in charge at the FSA and the Directors-General of Local Finance Bureaus having jurisdiction over the location of the business office, etc. pertaining to the issuance business of said Issuer of Prepaid Payment Instruments.

(3) In the case of an order to suspend business (Article 26 and Article 27(1) of the Act)

When issuing an order to suspend business, the Director-General of the Local Finance Bureau shall send relevant materials to the department in charge in the FSA and the Directors-General of Local Finance Bureaus having jurisdiction over the location of the business office, etc. pertaining to the issuance business of said Issuer of Prepaid Payment Instruments.

(4) In the case of a disposition to revoke registration (Article 27 of the Act)

When revoking the registration of an Issuer of Prepaid Payment Instruments, the Director-General of the Local Finance Bureau shall send relevant materials to the divisions in charge at the FSA and other Local Finance Bureaus. If said Issuer of Prepaid Payment Instruments is a corporation, the Director-General of the Local Finance Bureau shall send materials relating to the names of its officers (or trade name or other name of the corporation) within 30 days prior to the date of rescission, as well.

Checklist for Examination for Registration of Issuer of Prepaid Payment Instrument for Third-Party Business
(controls necessary to comply with the provisions of this Chapter)

Applicant name: _____

Note: Fill in "–" for "Not Applicable".

Examiner:

Date of Examination: YY/MM/DD

Applicability	Points to check
	Internal rules concerning the business of issuing Prepaid Payment Instruments or other documents equivalent thereto (Article 16(viii) of the Cabinet Office Order)
	Basic Policy on Compliance, etc. (II-1-1)
☐	Is the division responsible for legal compliance specified?
☐	Has a basic policy on compliance been established?
☐	Has a specific implementation plan (compliance program) been established?
☐	Has a code of conduct (Code of Ethics and Compliance Manual) been established?
☐	Does the applicant verify whether the business of issuing Prepaid Payment Instruments is conducted in compliance with laws and regulations and in an appropriate manner, for example, by conducting monitoring and verification by the Internal Control Department and internal audit by the Internal Audit Department?
	Prevention of Damage that May be Inflicted by Anti-Social Forces (II-1-2)
☐	Is the management team of the applicant properly involved in banning of relationships with antisocial forces? Is there a policy calling for firm-wide response?
☐	Has the applicant established a division in charge of supervising responses to ban any relationship with anti-social forces so as to develop a centralized control environment for preventing infliction of damage by anti-social forces?
☐	Does the Issuer of Prepaid Payment Instruments take measures to ban allowing anti-social forces to become a counterparty to a transaction including member shops, by conducting appropriate advance screening using information, etc. on anti-social forces to prevent transactions with anti-social forces, and making sure to insert provisions regarding the exclusion of organized crime group in all contracts and terms of transactions?
☐	Has the Issuer of Prepaid Payment Instruments established a framework for conducting an appropriate follow-up review on existing contracts for the purpose of making sure that any relationships with anti-social forces are eliminated?
☐	Does the applicant, with the appropriate instructions and involvement of the management team, encourage termination of transactions with anti-social forces in close cooperation with external expert organizations such as the police, the Center for Removal of Criminal Organizations, and lawyers on an ongoing basis? In addition, does the applicant take care not to provide benefits to antisocial-forces when canceling transactions?
☐	When anti-social forces make unreasonable demands, does the applicant cope with them with the appropriate instructions and involvement of the management team, and proactively consult with external expert organizations such as the police, the Center for Removal of Criminal Organization, and lawyers?
☐	Does the Issuer of Prepaid Payment Instruments manage shareholder information properly, through means such as regularly checking the transaction status of its own shares and examining information regarding the attributes of its shareholders?
	Actions to Misconduct (II-1-3)
☐	Is the division responsible for dealing with misconduct cases specified?
☐	Has the applicant established measures to be taken when misconduct is found?
	Obligation to Provide Information (II-2-1)
☐	Has the division responsible for the provision of information based on Article 13 of the Act been clarified?
☐	Does the applicant appropriately provide users with information on matters specified in each item of Article 13(1) 1 of the Act?
☐	Also, is it possible for a user to check such information even after purchasing the Prepaid Payment Instruments?
☐	Does the applicant provide users of Prepaid Payment Instruments with the matters prescribed in each item of Article 23-2(1) of the Cabinet Office Order without omission?
	Books and Documents (II-2-2)
☐	Is the division responsible for preparing books and documents specified?
☐	Has the applicant developed a control environment for properly preparing and preserving books pertaining to the business of issuing Prepaid Payment Instruments?
☐	Does any department, such as the Internal Audit Department, other than the books-and-documents-preparation division, verify the accuracy of the description of the books and documents?
☐	In cases where books are prepared electronically, is there a control environment in which books can be restored when data are damaged, for example, via periodic back-up of books, etc.?
	Control Environments for Management of User Information (II-2-3)
☐	Is the division responsible for managing user information specified?
☐	Does the management team endeavor to develop an internal control system, such as establishing an organizational system and formulating internal rules to ensure the appropriateness of the management of user information?
☐	Has the applicant formulated a specific standard for the handling of user information and communicated it to all officers and employees through the provision of training and other means?
☐	Has the applicant established a control environment that enables timely and appropriate verification of the status of management of user information?

Applicability	Points to check
☐	Has the applicant taken appropriate measures for preventing wrongful acts utilizing user information, such as the dispersal of authority concentrated upon specific personnel and the enhancement of controls and checks over personnel who have broad powers?
☐	Has the applicant established frameworks for appropriately reporting to responsible divisions when user information has been leaked, and notifying relevant users, reporting to the relevant authorities, and disclosing to the public in a prompt and appropriate manner to prevent secondary damage?
☐	Does the applicant analyze the causes of information leaks and implement measures designed to prevent recurrence?
☐	In light of incidents of information being leaked at other companies, does the applicant examine measures needed to prevent a similar incident from occurring in its organization?
☐	Does the applicant conduct audits covering the broad range of business operations handling user information by its independent Internal Audit Department on a periodic or as-needed basis?
☐	Has the applicant implemented appropriate measures, such as training programs, in order to increase the specialization of the staff engaged in audits pertaining to the management of user information?
☐	With regard to information concerning individual users, has the applicant implemented the following measures pursuant to Article 44 of the Cabinet Office Order? (Necessary and appropriate measures concerning safety management) (A) Measures based on Article 8 of the Financial Sector Personal Information Protection Guidelines (B) Measures based on I, and Appendix 2 of the Practical Guidelines (Necessary and appropriate measures concerning supervision of employees) (C) Measures based on Article 9 of the Financial Sector Personal Information Protection Guidelines (D) Measures based on II of the Practice Guidelines
☐	Has the applicant implemented measures to ensure that sensitive information of individual users is not used except for the cases specified in each item under Article 5(1) of the Financial Sector Personal Information Protection Guidelines?
☐	For credit card information, etc., has the applicant implemented the following measures? (A) Has the applicant set an appropriate period of time for keeping credit card information, etc., which takes into account the purpose of use and other circumstances, and does it limit the locations where such information is kept, and dispose of the information in a prompt and appropriate manner after the retention period has lapsed? (B) Has the applicant implemented appropriate measures when displaying credit card information, etc. on computer monitors, such as not displaying whole credit card numbers, unless needed for business operations? (C) Does the independent Internal Audit Department of the applicant conduct internal audit on a periodic or as-needed basis on whether the rules and systems for protecting credit card information, etc. are functioning effectively?
	Control Environment for Complaint Processing (II-2-4)
☐	Is the division responsible for handling complaints specified?
☐	Has the applicant established a division in charge of complaints, etc. and procedures for processing them so that complaints, etc. can be processed and dealt with promptly and appropriately?
☐	Does the Issuer of Prepaid Payment Instruments have a system for sharing information among relevant parties as necessary according to the case, such as reporting to the Internal Audit Department and the management team if a complaint, etc. could have a material impact on the management thereof?
☐	With regard to complaints, etc. pertaining to the use of Prepaid Payment Instruments at member shops, has the applicant developed an appropriate complaint consultation system, such as a system to accept direct communication from users to the Issuer of Prepaid Payment
☐	Has the applicant developed a control environment for sincerely responding to complaints, etc., such as providing sufficient explanations to users, obtaining their understanding and consent, and resolving them?
☐	Has the applicant appropriately followed up the status of responding to complaints, etc.?
☐	Does the applicant properly and accurately record and keep the contents of complaints, etc. and results of measures taken therefor? Also, has the applicant developed a control environment wherein it analyzes the contents of complaints, etc. and the result of handling them, and applies this on an ongoing basis to the improvement of control environments for dealing with users and conducting administrative processes and to the formulation of measures for preventing any occurrence or recurrence of complaints?
	Measures to Prevent Inappropriate Use (II-2-6)
☐	Has the upper limit of transferable unused balance of Prepaid Payment Instruments been set to a reasonable amount according to actual demand, in order that it will not be used for inappropriate transactions?
☐	Has the applicant developed a system for detecting suspicious transactions, such as identifying those who have repeatedly received transfers of a certain amount or more?
☐	Has the applicant taken measures such as temporarily suspending the use of transactions with persons who are engaged in suspicious transactions? Also, does the applicant check parties involved in such suspicious transactions and the content thereof as needed?
	Responses to Persons with Disabilities (II-2-7)
☐	Has the applicant developed an internal control environment for taking appropriate measures in accordance with the Disability Discrimination Act and the Guidelines for Eliminating Discrimination against Persons with Disabilities?

Applicability	Points to check
	Linkage with Services Provided by Other Service Providers such as Account Transfer Service (II-2-8)
☐	Does the management team have the Internal Control Department identify inherent risks with regard to the entire collaborative services at the time of introduction thereof or at the time of any change in the contents and methods thereof, and develop a system to reduce risks in a timely manner based on these?
☐	Does the Internal Control Department collect and analyze information on the occurrence of related crimes and methods thereof in collaborative services, and improve the system for the operation of collaborative services (including fraud prevention measures)? Also, does it report the content thereof to the management team on a regular and timely basis?
☐	Does the Internal Audit Department audit the control environment (including fraud prevention measures) for the operation of collaborative services on a regular and timely basis? Also, does it report the audit result to the management team?
☐	Does the management team create an environment in which the so-called PDCA cycle, which consists of risk analysis, the formulation and implementation of risk mitigation measures, and the evaluation and review thereof, functions as described above?
☐	Does the applicant assess possible risk of the entire collaborative service in cooperation with its business partners at the time of introduction thereof or at the time of any change in the contents and methods thereof? Also, does it cooperate with the business partners in assessing the risk?
☐	Has the applicant clarified the division of roles and responsibilities with the business partners?
☐	Based on the risk assessment, does the applicant crosscheck information on users in cooperation with the business partners, and take appropriate and effective measures commensurate with risks to prevent fraud? For example, in the case of linking with an account transfer service, does the applicant take appropriate and effective measures to prevent unauthorized use, such as notifying depositors at the linked bank accounts via their telephone numbers and addresses registered therewith of information necessary for authentication by the Issuer of Prepaid Payment Instruments and setting the charge limit at a level that is deemed to enable prevention of improper transactions?
☐	Has the applicant confirmed that partner banks, etc. that offer the account transfer services have introduced multi-factor authentication and other authentication methods that combine effective elements? * It should be noted that fraud prevention measures taken by an Issuer of Prepaid Payment Instruments do not overlap with those taken by the partner banks, etc.
☐	Does the applicant regularly and in a timely manner check and re-evaluate risks in light of changes in the environment, including the sophistication of crime methods, and the occurrence of incidents at the applicant itself or other business operators, and improve measures to prevent fraud, including the introduction of public personal authentication?
☐	If, as a result of risk assessment, it is found that there is a problem, does the applicant temporarily suspend all or part of its services, including collaborative services, or take other appropriate measures until the problem is resolved?
☐	When engaging in the linked account transfer service, etc., with business partners, does the applicant take measures to enable users, etc. to confirm the fact that such service is a collaborative service and the content of such service in a timely manner by cooperating with the partner to notify users, etc. at their contact information such as the telephone number and e-mail address registered with the partner in advance, so that users, etc. can be aware of fraud or other damage, if any, at an early stage?
☐	With regard to the collaborative services, from the viewpoint of preventing improper transactions, has the applicant developed a control environment for appropriately implementing the following matters, for example, in cooperation with business partners? • To promptly detect transactions suspected of being fraudulent by setting appropriate scenario or thresholds based on changes in the environment, including the sophistication of criminal methods, and the occurrence of incidents in it or other business entities • To share information on suspicious transactions detected based on the above with partners in a timely manner, to take necessary measures including suspension of the services, and to investigate such suspicious transactions • To promptly notify persons who may be a victim of fraud of the incident • To suspend the use of IDs that have been confirmed to be used for improper transactions
☐	Has the applicant developed a control environment for accumulating and analyzing cases of inquiries and consultations from users, etc. concerning collaborative services (hereinafter referred to as "inquiries, etc.") and utilizing them for early detection of risks, and for improvement of fraud prevention measures and responses to consultations from users, etc.?
☐	Has the applicant developed a control environment for honestly and sincerely responding to users, including inquiries, etc. on business partners? Also, has it clarified how to cooperate and share the responsibilities with business partners in specific manners?
☐	Does the applicant crosscheck with a business partner whether each of them has taken any inappropriate actions in responding inquiries, etc. form users, such as inducing users, etc. who made an inquiry to either party to contact the other party? And if any inappropriate actions are found, does the applicant, together with the partner, properly investigate the cause thereof, and take corrective measures and measures to prevent recurrence, etc.?

Applicability	Points to check
	Compensation for Damage due to Improper Transactions (II-2-9)
☐	Has the applicant formulated a policy concerning compensation for damage arising from improper transactions conducted in connection with the business of issuing Prepaid Payment Instruments and other measures (hereinafter referred to as "Compensation Policy")? And has it provided users of Prepaid Payment Instruments with necessary information and made it available also to persons other than the users of Prepaid Payment Instruments who are likely to incur losses in the event of the occurrence of improper transactions?
☐	Does the Compensation Policy include at least the following items? (A) Depending the contents of business of issuing Prepaid Payment Instruments, whether or not compensation for damage is to be provided to victims for each specific situation in which damage is likely to occur, and the content of and requirements for compensation, if any (B) Content of the compensation procedure (C) In cases of collaborative services, particulars concerning the sharing of compensation between the Issuer of Prepaid Payment Instruments and the partner (including those who provide compensation to victims) (D) Inquiry and contact for compensation (E) Standards for disclosure of improper transactions
☐	Has the applicant developed a control environment for appropriately and promptly providing compensation in accordance with the established Compensation Policy (in the case of collaborative services, including a system for cooperation with business partners)?
☐	Does the applicant share necessary information with business partners (if any) and the Certified Association for Payment Service Providers (if it is a member thereof), etc. concerning risks of improper transactions and actual cases thereof, such as inquiries, etc. from users, etc. concerning improper transactions?
	IT Systems Management (II-3-1)
☐	Is the division responsible for managing IT system specified?
☐	Does the applicant conduct periodic reviews and formulate basic policies for the IT system risk management as needed?
☐	Has the applicant developed a control environment for preventing IT system failures, etc. and for quick recovery measures in the event of such failures?
☐	Has the applicant appointed an officer who oversees and manages IT systems?
☐	Has the applicant determined specific measures to take in case of crisis where an IT system failure, etc. occurs?
☐	Has the applicant established the basic policy for managing the IT system risk?
☐	Does the basic policy for managing the IT system risk contain the security policy (a basic policy for proper protection of information assets of an organization) and the policy on outsourced contractors?
☐	Does the division in charge of managing IT systems identify and manage the upper limit of the transactions through the computer system and consider system and administrative measures for cases where the transactions exceed the upper limit?
☐	Has the applicant developed an IT security management system for the appropriate management of information assets and has the applicant been making efforts for continuous improvement through the PDCA cycle?
☐	Does the applicant manage information by designating individuals responsible for information security and clarifying their roles/responsibilities?
☐	Has the applicant established information management rules and introduced a mechanism to prevent information leakage, etc., according to each of the important information items of users that have been thoroughly identified, after conducting importance assessment and risk assessment?
☐	Does the applicant give due consideration to the necessity of confidential information for business purposes and treat such information in a stricter manner?
☐	Does the applicant periodically monitor its information assets to see if they are managed properly according to management rules, etc., and review the control environment on an ongoing basis?
☐	Are measures taken in case of data loss?
☐	Has the applicant developed a necessary control environment, such as the establishment of an organizational structure and the formulation of internal rules, while recognizing the importance of cybersecurity?
☐	Has the applicant introduced a multi-layered defense system against cyberattacks that combines security measures respectively for inbound perimeter control, internal network security control, and outbound perimeter control?
☐	Has the applicant taken measures to prevent expansion of damage when cyberattacks occur?
☐	Are necessary measures introduced for vulnerabilities in the IT system, such as updating of the operating system and application of security patches, in a timely manner?
☐	Does the applicant regularly evaluate the level of cyber security and improve security
☐	When conducting non-face-to-face transactions using communication means such as the Internet, has the applicant introduced an appropriate authentication method suited to transaction risks, such as multi-factor authentication that combines effective elements such as variable passwords, biometric authentication, and electronic certificates, or an authentication method that does not rely solely on fixed IDs and passwords, or a transaction authentication method that uses multiple routes?
☐	When conducting non-face-to-face transactions using the Internet and other means of communication, has the applicant taken anti-fraud measures corresponding to the business? Also, has the applicant established a system to detect illegal logins, abnormal transactions, etc., and to promptly notify such anomalies to the user, and to suspend the use of IDs confirmed as unauthorized?
☐	Are rules to authorize plans, development, and transitions of IT system development projects clearly established?

Applicability	Points to check
☐	Does the Internal Audit Department (or external auditor), which is independent from the IT Systems Department, conduct periodic audits of IT systems?
☐	Has the applicant established criteria for selecting outsourced contractors (including IT system-related subsidiaries)?
☐	Does the applicant, in entering an outsourcing contract with an outsourced contractor, set out division of roles and responsibilities between them, supervising authority to audit outsourced work, subcontracting procedures, rules and security requirements to be observed by the officers and employees of the outsourced contractor in the contract?
☐	Is risk management carried out properly in outsourced IT system work (including multi-tiered outsourcing)?
☐	In cases where IT system-related administrative work is outsourced to contractors, too, does the applicant properly manage the risk thereof in the same manner as outsourcing of IT system [illegible]?
☐	Does the applicant, as an outsourcer, regularly check and monitor to confirm that outsourced work (including multi-tiered outsourcing) is carried out appropriately?
☐	Has the applicant formulated a contingency plan and established arrangements and procedures for dealing with emergencies?
☐	Does the applicant regularly conduct a drill based on its contingency plan? Also, is the drill conducted jointly with outsourced contractors and IT system partners according to the degree of importance and risk?
☐	For important systems whose failure could seriously affect business operations, has the applicant developed a control environment to address disasters, IT system failures, etc. so that normal business operations can be speedily brought back?
☐	Has the applicant clarified reporting procedures and the framework of command and supervision covering outsourced contractors in preparation for IT system failures, etc.?
☐	Has the applicant established measures to respond to users in the event of IT system failure, etc.?
Administrative Risk Management (II-3-2)	
☐	Is the division responsible for managing administrative risk specified?
☐	Also, has the applicant established rules and regulations regarding administrative work and processes?
☐	Does the Internal Audit Department properly conduct internal audits in order to examine the control environment for managing administrative risk?
☐	Has the division in charge of managing administrative risk at headquarters taken measures for checking business offices' control environment for managing administrative risk?
Outsourcing (II-3-3)	
☐	Has the applicant established internal rules, etc. specifying criteria for selecting contractors, or measures to be taken when outsourcing risk appears, and disseminated such rules, etc. through internal training, etc.?
☐	Has the applicant established a control environment for taking appropriate measures, such as issuing necessary instructions regarding the development of a legal compliance system at the outsourced contractor?
☐	Has the applicant taken measures to ensure that outsourcing does not hinder the performance of obligations to supervisory authorities regarding inspections, reporting orders, submission of records, etc.?
☐	Has the Issuer of Prepaid Payment Instruments implemented measures to ensure that it makes clear that the outsourcing of business operations does not cause any change in the contractual rights and obligations involving it and its users and that the users continue to have the same rights as if the business operations were conducted by the Issuer of Prepaid Payment Instruments itself?
☐	In the case of outsourcing the operation relating to cash payment and receipt with users, when the outsourced contractor receives and pays cash from or to users, has the applicant taken measures to appropriately identify increases and decreases in the unused balance pertaining to the receipt and payment of cash?
☐	Has the Issuer of Prepaid Payment Instruments developed a control environment that prevents users from suffering inconveniences if it cannot be provided the services agreed under the outsourcing contract with its outsourced contractor?
☐	When outsourcing the handling of information of individual users to an outsourced contractor, has the applicant taken the measures to supervise the outsourced contractor as necessary and appropriate measures to prevent such information from being leaked, lost, or damaged based on Article 10 of the Financial Sector Personal Information Protection Guidelines and III of the Practice Guidelines?
☐	Does the applicant clarify the division responsible for the management of outsourcing and monitor how business operations are being conducted at outsourced contractors, on a regular basis or as needed?
☐	With regard to complaints, etc. pertaining to the outsourced service, has the applicant developed an appropriate complaint consultation system, such as a system to accept direct communication from users to the Issuer of Prepaid Payment Instruments, who is the entrustor of such service?
☐	Does the applicant confirm that outsourced contractors properly manage user information?
☐	Has the applicant confirmed that outsourced contractors have systems in place to take appropriate actions and to promptly report to the applicant in the event that information is leaked, lost, or damaged at outsourced contractors?
☐	Does the applicant restrict the access right by outsourced contractors to user information possessed by the applicant to the extent necessary according to the nature of the outsourced business?
☐	In cases of multi-tiered outsourcing, does the applicant check whether the outsourced contractor is adequately supervising such subcontractors? And does it directly supervise the subcontractors and other business operators as needed?
Refunds of Prepaid Payment Instruments (II-3-4)	
☐	In cases where a refund is to be made pursuant to Article 20(5) of the Act, has the applicant developed a control environment for preventing refunds from exceeding the upper limit specified by laws and regulations?
☐	In cases where a refund is to be made pursuant to Article 20(5) of the Act, does the applicant provide appropriate explanations to users about the refund procedure?
Management of Member Shops (II-3-5)	
☐	When concluding a member shop contract, does the applicant confirm whether or not the counterparty is engaging in suspicious business in light of public order and morals?
☐	If it is found that there is a problem in the business of a member shop in light of public order and morals after the conclusion of the member shop contract, is it possible to promptly cancel the contract?
☐	With regard to the details of goods and services sold or provided by the member shop to users, has the applicant developed a control environment that enables it to identify any significant change in the matters confirmed at the time of the conclusion of a member shop contract?
☐	Does the applicant require each member shop to report on the use of Prepaid Payment Instruments at regular intervals? Also, does it have a control environment in which a department different from the department that manages the usage records of member shops verifies the accuracy of the reported payment amounts?