May 1, 2017

Company Name: GMO Payment Gateway, Inc.
Representative: Issei Ainoura
President & Chief Executive Officer
Code: 3769 (TSE First Section)
Contact: Ryu Muramatsu
Executive Vice President
(TEL. +81-3-3464-0182)

Notice of the Investigation Report of the Recurrence Prevention Committee

As announced in “Apology and Report for Leak of Personal Information Due to Unauthorized Access” dated March 10, 2017 and “Establish of ‘Recurrence Prevention Committee’” dated March 14, 2017, unauthorized access by a third party to the payment sites of our consignment merchants, Tokyo Metropolitan Government credit card payment site for metropolitan tax (“metropolitan tax payment site”) and credit card payment site for group life insurance rider of Japan Housing Finance Agency (“insurance rider payment site”) was confirmed, and credit card information and personal information of the users were leaked from both sites. In this regard, the Company established the Recurrence Prevention Committee whose members include external experts effective March 14, 2017, based on the decision that it needs objective, specialized, impartial and transparent investigation, examination and judgment for the investigation of the facts and cause of the incident and development of recurrence prevention measures, and the Committee conducted the investigation of the incident as well as discussed and implemented the recurrence prevention measures until April 30, 2017.

We hereby give notice that the “Investigation Report on Information Leak Due to Unauthorized Access” was compiled and submitted by the Recurrence Prevention Committee to the Board of Directors of the Company.

As of now, there is no report on any improper use of the credit card information acquired illegally.

We would like to express our sincerest apologies for causing tremendous inconvenience and concerns to our customers, shareholders, investors, market players and all other related parties.

1. The investigation report of the Recurrence Prevention Committee

   The overview of the investigation report is as follows. Please refer to the accompanying “The Investigation Report on Information Leak Due to Unauthorized Access” for more detail.

   (1) Overview of the incident

   From March 8 to March 9, 2017, at the metropolitan tax payment site and the insurance rider payment site, our consignment merchants, the vulnerability of Apache Struts 2, an application framework, (vulnerability which enables remote execution of any command (S2-045)) was exploited, and a back door program was set up inside the server, through which encrypted data including credit card information and personal information of the site users were illegally obtained by an attacker.

   (2) Recurrence prevention measures

   The Recurrence Prevention Committee decided to implement short-term and mid- and long-term technical prevention measure and the prevention measure regarding information security management. Please refer to Ⅶ Recurrence Prevention Measures of the accompanying “The Investigation Report on Information Leak Due to Unauthorized Access” for more detail.

(3) Implementation of the recurrence prevention measures

Based on the recurrence prevention measures decided at the Recurrence Prevention Committee, the Company implemented the following preventive measures before April 14, 2017.

(i) Short-term technical preventive measures
(ii) Reconsideration of procedures for security incident reporting
(iii) Revision of guidelines regarding system development process

In addition, as efforts to relaunch the metropolitan tax payment site and to prevent recurrence, the Company conducted PCI DSS assessment by Payment Card Forensics, Inc. on the metropolitan tax payment site and the insurance rider payment site. As a result, it was confirmed that they satisfy the PCI DSS requirements as of April 14, 2017.

2. Management responsibility

As described in the investigation report of the Recurrence Prevention Committee, the incident was caused by the information security management system and its operation. We take this incident seriously and decided to take the following actions in order to make clear the management responsibility.

Issei Ainoura, President & Chief Executive Officer	30% monthly salary cut for three months
Satoru Isozaki, Executive Vice President	30% monthly salary cut for three months
Shinichi Sugiyama, Director	10% monthly salary cut for one month

Investigation Report on Information Leak Due to Unauthorized Access

April 30, 2017

GMO Payment Gateway, Inc.

Recurrence Prevention Committee

Table of contents

Glossary of Terms

For the purpose of this report, terms and abbreviations shall be defined as follows.

Index	Terms	Description
G	GMO-PG	GMO Payment Gateway, Inc.
I	IPA	Information-technology Promotion Agency
	ISMS	Information Security Management System: Comprehensive framework to manage and protect information assets appropriately
J	JPCERT	Japan Computer Emergency Response Team: General incorporated association engaging in collection and transmission of computer security information and incident response support
P	PCF	Payment Card Forensics, Inc.,
	PCI DSS	Payment Card Industry Data Security Standard: The global security standard jointly formulated by international credit card companies to protect credit card information securely
W	WAF	Web Application Firewall: A type of firewall. Software or equipment that monitors contents of application correspondence, and monitors and blocks illegal correspondence
	Application framework	A group of software that aggregates functions and processing necessary for application in certain domain as parts
	Recurrence Prevention Committee	Committee which includes external specialists and is established for the purpose of investigating the facts and causes of the Incident and presenting recommendations for recurrence prevention measures
	Information Security Committee	Committee established within the Company in accordance with the information security control rules of GMO-PG in order to manage and implement information security
	Backdoor program	A malicious program that creates a backdoor that allows remote access to a system without proper procedures
	Firewall	Software or equipment that controls monitoring and blocking of correspondence at the border of internal network and outside
	Forensic investigation	Investigation to reveal facts by analyzing tracks and logs left on the system after unauthorized access

	PrivacyMark	PrivacyMark System is a system set up to assess private enterprises that take appropriate measures to protect personal information. The System is in compliance with Japan Industrial Standards (JIS Q 15001:2006 [Personal Information Protection Management System - Requirements]).
	Division	Body managing the business of GMO-PG https://corp.gmo-pg.com/company/figure/
	Risk Management Committee	Committee established within the Company in accordance with the risk management rules of GMO-PG in order to manage the enterprise risk

I. Overview of the Investigation

1. Background of establishment of the Recurrence Prevention Committee

On March 9, 2017, based on the information provided in “Countermeasures for vulnerability of Apache Struts 2 (CVE-2017-5638) (S2-045)” by Information-technology Promotion Agency (IPA) and “Alert on vulnerability of Apache Struts 2 (S2-045)” by Japan Computer Emergency Response Team (JPCERT), GMO-PG started an investigation of the effect on its system and confirmed that there was an unauthorized access by a third party at the payment sites of its consignment merchants, Tokyo Metropolitan Government credit card payment site for metropolitan tax (“**Metropolitan Tax Payment Site**”) and credit card payment site for group life insurance rider of Japan Housing Finance Agency (“**Insurance Rider Payment Site**”) and that the incident in which personal information of users of both sites was leaked (“**Incident**”) occurred.

The Company established the Recurrence Prevention Committee consisting of some external specialists effective March 14, 2017, based on the decision that it needs objective, specialized, impartial and transparent investigation, examination and judgment to investigate the facts and causes of the Incident, clarify where responsibility lies, and develop recurrence prevention measures.

Members of the Recurrence Prevention Committee are as follows:

Position	Name	Attribute
Chairman	Issei Ainoura	President & Chief Executive Officer
Member	Ryu Muramatsu	Executive Vice President
Member	Satoru Isozaki	Executive Vice President
Member	Yuichi Hisada	Managing Director
Member	Yasuhiko Kimura	Director
Member	Shinichi Sugiyama	Director
Member	Masaru Yoshioka	Director
Member	Yoshinobu Nakamura	Attorney-at-law of Yoshinobu Nakamura Law Office,
Specialist Advisor	Tetsuya Oi	Attorney-at-law of TMI Associates
Specialist Advisor	Kuniyoshi Shirai	Professor at the Graduate School of Information & Communication,
Specialist Advisor	Takayuki Okochi	Forensic Senior Consultant of PCF

2. The purpose of the investigation

The report was prepared based on the investigation conducted until April 30, 2017 in order to report on the Recurrence Prevention Committee's opinion regarding the delegated matters as described below as of the date of submission of the report.

It should be noted that the report represents the Recurrence Prevention Committee's opinion on the delegated matters from an objective perspective in light of the GMO-PG's purpose of establishing the Committee.

3. Delegated matters

The matters delegated to the Recurrence Prevention Committee are:

(1) the factual investigation of the Incident;

(2) the investigation of the causes of the Incident; and

(3) recommendations of the recurrence prevention measures.

4. Investigation period

From March 14, 2017 to April 30, 2017

5. Investigation method

In preparing the report, the Recurrence Prevention Committee conducted an investigation within the range of the information disclosed during the above-mentioned period through the following methods, on the premise that such information is true and accurate.

(1) Investigation by interview

(2) Review of documents including company rules

(3) Investigation of various logs

(4) On-site technical investigation

Sections from II to VI set forth below are the report by external specialist advisors in the Recurrence Prevention Committee and does not include information that may become a security risk.

II. Overview and Background of the Incident

1. Summary of the Incident

GMO-PG acquired PCI DSS certification for the first time in December 2008, passed an annual recertification audit eight times since then, and acquired the latest certification in December 2016, which means that the Company maintained a certain level of information security system required for a business operator handling credit card information. However, the Incident occurred because the security system did not work against the zero-day attack exploiting new vulnerabilities of Apache Struts 2.

Given the materiality of the vulnerability risk of Apache Struts 2, GMO-PG made the “Stop-using-Struts policy” to suspend the use of Apache Struts 2 in April 2016 and has not used it in new systems since then.

On the other hand, measures for certain existing systems were limited only to apply patches of Apache Struts 2, considering the significance of the impact of the system change and on customer operations. So GMO-PG was attacked before these measures were taken place.

It is still required, however, to make a perpetual effort to build more robust information security system by improving the system to collect vulnerability information early, enhancing ability to detect unauthorized operation, improving countermeasures against data cover-up and improving a process to build a security-conscious system. To this end, the Recurrence Prevention Committee, in addition to the investigation of the causes of the Incident, reviewed GMO-PG’s overall information security system thoroughly and recommended implementation of multi-layered security measures to ensure prevention of recurrence.

2. Acquisition of certification related to the business affected by the Incident

GMO-PG acquired its first ISMS certification in April 2006, passed a triennial recertification audit for three times, and acquired the latest certification in December 2014. ISMS requires its member companies to receive a recertification audit every three years and also receive an external surveillance audit annually, which GMO-PG also received.

In addition, GMO-PG acquired its first PCI DSS certification in December 2008, passed an annual recertification audit for eight times, and acquired the latest certification in December 2016.

Moreover, GMO-PG acquired its first PrivacyMark in September 2009, passed a biennial audit for three times, and acquired the latest PrivacyMark in September 2015.

3. Overview of the Incident

From March 8 to March 9, 2017, at the Metropolitan Tax Payment Site and the Insurance Rider Payment Site, GMO-PG's consignment merchants, the vulnerability of Apache Struts 2, an application framework, (vulnerability which allows remote execution of arbitrary commands (S2-045)) was exploited, and a backdoor program was set up inside the server, through which encrypted data including credit card information and personal information of the site users were illegally obtained by an attacker.

4. Time series from detection to initial response

Date	Time	Event	personnel in-charge in GMO-PG
March 6	22:14	US Apache Site announced the vulnerability (S2-045), at which time, Max Security Level was High and subsequently changed to Critical at 5:59 on March 20.	
March 7	15:21	Github disclosed the attack code.	
March 8	04:54	An attack to the Insurance Rider Payment Site started.	
	04:57	A backdoor program was set up at the Insurance Rider Payment Site.	
	10:43	JPCERT sent early alert information.	(Note) GMO-PG was not a member of JPCERT at this point.
	15:25		Received an e-mail about the vulnerability information from an external security information providing service.
	16:51	An attack to the Metropolitan Tax Payment Site started.	
	17:14	A backdoor program was set up at the Metropolitan Tax Payment Site.	
	17:40	Unauthorized access to the Metropolitan Tax Payment Site Database started.	
	18:20	An application exception was detected in the Metropolitan Tax Payment Site Database.	Determined it as illegal attack and blocked the attacker's IP with the firewall.

	23:53	Unauthorized access to the Metropolitan Tax Payment Site Database was terminated.	
March 9	02:30	Unauthorized access to the Insurance Rider Payment Site Database started.	
	04:59	Unauthorized access to the Insurance Rider Payment Site Database was terminated.	
	18:00	Perceived IPA’s alert on the vulnerability.	Recognized the vulnerability information.
	21:56		Blocked the attack related to the Incident with WAF.
	22:40		Established Emergency Taskforce.
	23:53		Shut down all systems running with Apache Struts 2 and switched to a backup system which was not connected to network.
March 10	00:30		Applied a patch for Apache Struts 2 to the above-mentioned backup system (to change the parser).
	02:15		Confirmed the trace of hacking and unauthorized access to Database at the Metropolitan Tax Payment Site and the Insurance Rider Payment Site.
	08:05		Notified the parties concerned and started discussion about the responses.
	09:20		Requested a forensic investigation to PCF.
	11:15	Stopped services of the Metropolitan Tax Payment Site.	
	11:30	Stopped services of the Insurance Rider Payment Site.	
	14:00		Started to share credit card information that might have been leaked with the relevant credit card companies to prevent secondary damage (completed at 19:30).
	17:00		Set up a special call center.
	18:22		Made announcement of the Incident on the website and timely disclosure.

III. Responses to the Incident

1. Assessment on collection of the vulnerability information

(1) Provision of the vulnerability information from an external contracting agency

Although GMO-PG received an e-mail about the vulnerability information (“E-mail”) from an external security information providing service at 15:25 on March 8, the security personnel did not confirm the content and failed to recognize the significance of the vulnerability information immediately.

(2) Assessment on collection of the vulnerability information

The vulnerability of Apache Struts 2 (“S2-045” or “CVE-2017-5638”) allows remote execution of arbitrary commands. Accordingly, any malicious third party could use this vulnerability to set up or delete a backdoor program via Internet. As for the collection of the vulnerability information by GMO-PG, the E-mail containing the vulnerability information was received at 15:25 on March 8, but the E-mail did not indicate the degree of risk. According to the log analysis in GMO-PG, the first backdoor program was set up at 4:57 on March 8, at which point the degree of risk was still not clear. Moreover, the notification by the E-mail was received two days after the vulnerability announcement by Apache Software Foundation, a developer of Apache Struts 2.

GMO-PG should have taken its own security measures based on the information provided by the developer, particularly when it used an open source software Apache Struts 2.

2. Assessment on the responses to the Incident

(1) Actions taken before and after the Incident was happened

GMO-PG detected the occurrence of an application exception at 18:20 on March 8, which was determined as an illegal attack, and the correspondence from the attacker’s IP address was immediately blocked with the firewall. The unauthorized access, however, continued until 23:53 on that day.

After the security personnel recognized the detailed information on the vulnerability of Apache Struts 2 at 18:00 on March 9, GMO-PG initiated the investigation based on such information and recognized the possibility of information leak at 20:00 on the same day. At 21:56 on the same day, GMO-PG implemented an emergency measure to shut down with WAF.

As described above, GMO-PG took certain initial response measures according to the practical proceudres.

(2) Establishment of the Emergency Taskforce and subsequent instructions on emergency measures

At 22:40 on March 9, the Emergency Taskforce was established in the head office.

Considering the threat posed by the vulnerability of Apache Struts 2, the GMO-PG's decision to promptly establish the Emergency Taskforce can be evaluated as important to centralize the chain of command within the Company and ensure to take top-down measures for priority matters.

(3) Process leading up to reporting to parties concerned and public announcement

GMO-PG completed the reporting of the Incident to various parties concerned including relevant authorities by March 10 as well as the notification to the Shibuya Police Station. In addition, for the purpose of preventing further damage by the Incident, GMO-PG stopped service of the Metropolitan Tax Payment Site and the Insurance Rider Payment Site at 11:15 and at 11:30 on March 10, respectively.

Moreover, in order to prevent secondary damage arising from the illegal use of the leaked information, GMO-PG started to share credit card information that might have been leaked with relevant credit card companies from 14:00 on the same day and set up a call center to cope with the Incident at 17:00 on the same day.

At 18:22 on the same day, GMO-PG made timely disclosure and announcement of the Incident on its website.

As described above, it can be evaluated that there was no delay in the process from the establishment of the Emergency Taskforce to the reporting to parties concerned and the public announcement.

IV. Results of the Forensic Investigation

1. Submission of the final report of the forensic investigation

On March 31, 2017, GMO-PG received the final report of the forensic investigation (“**Final Report**”) from PCF. GMO-PG immediately started the implementation of the prevention measures including those recommended in the Final Report.

V. Information Security Management System

1. Information security incident management

(1) Gathering information on vulnerability and inadequate response system for vulnerability

GMO-PG has the internal rules providing for response procedures for security incidents, and therefore, in case any vulnerability is detected, such fact shall be reported to the Information Security Committee Administrative Office, which issues instructions for subsequent responses.

However, the only means for GMO-PG to collect information on vulnerability was to receive information from the outside security information providing service. In addition, even though there are rules for procedures to handle vulnerability information collected, there was a lack of well-defined procedures for the relevant personnel to follow that crystallize the procedures to escalate information, such as a checklist, flowchart or contact lists.

2. System development process

(1) System development related to the Incident

(a) Recognition of risk associated with the use of Apache Struts 2

GMO-PG used Apache Struts 2 for the first time for an automobile tax payment site of a local government around 2010. Subsequently, the Company applied the similar method to other entrusted construction of a credit card payment site system for taxes other than automobile tax, and therefore, the Company also used Apache Struts 2 for the Metropolitan Tax Payment Site.

On the other hand, the Insurance Rider Payment Site had many differences with the Metropolitan Tax Payment Site in terms of screen transition and required new construction of many parts, but Apache Struts 2 was used for the system construction.

From 2013 to 2014, when many incidents of unauthorized access exploiting the vulnerability of Apache Struts 2 were reported in various areas, GMO-PG did not come to a decision to replace Apache Struts 2 with other software because the Company was able to prevent unauthorized access by responding to each vulnerability information related to Apache Struts 2. Around the autumn in 2014, security personnel and development personnel of GMO-PG started to consider and discuss suspending the use of Apache Struts 2 due to the significance of the risk posed by its vulnerability. However, the risk of using Apache Struts 2 in the existing system was never escalated to the management on the ground that suspending the use of Apache Struts 2 and making changes to the existing system would have significant impacts on parties concerned such as customers.

In recent years, there have been cases where countermeasures against the vulnerability attack do not work adequately as the methods of attack have become diversified and sophisticated, and if the system is in fact attacked, the impacts caused by unauthorized access would be quite serious as described above. Nevertheless, GMO-PG did not have sufficient understanding of the risk posed by the vulnerability of Apache Struts 2, but clearly, should have discussed it more carefully within the Company.

After the “Stop-using-Struts policy” to suspend the use of Apache Struts 2 in April 2016, GMO-PG started construction of new systems without dependence on Apache Struts 2, but did not reconstruct the existing system using Apache Struts 2.

(b) Store the card verification code at the Insurance Rider Payment Site

Generally, code review is performed by members not involved in coding. In developing the Insurance Rider Payment Site, however, members who constructed the online section were also involved in coding and performed code review. In addition, verification after code review was insufficient at the Insurance Rider Payment Site, and as a result, card verification code was stored unexpectedly.

In order to develop a security-conscious system, security personnel and development staff need to work closely together in such a way that security personnel sets the secure coding standards and ensures development personnel complies with them, and also carry out the problem solving process which includes sharing and assessing development issues, and discussing and implementing measures to solve them.

Although GMO-PG shares information on vulnerability of individual applications and systems at its monthly meeting, there was not enough cooperation between security personnel and development personnel with regard to the development of security-conscious systems and the above-mentioned problem solving process was not adequately carried out.

VI. Corporate Risk Governance and Corporate Culture

1. Issues related to enterprise risk management

(1) Process to identify risks and select material risks

Generally, the enterprise risk management process should consist of identification and assessment of enterprise risk at the top management. In GMO-PG, the Risk Management Committee simply confirmed the risk assessment results of each division, and did not properly verify risks with a bird’s-eye view. Moreover, the Risk Management Committee was held only once a year, which made it difficult to perform risk monitoring in ordinary times or respond promptly to changes in quantity of risk.

The assessment of individual risks consists only of a qualitative assessment of the impact and frequency performed by each division, and changes in quantity of risk lacks objectivity. The risk of “detection of large-scale vulnerability” which can be considered as the cause of the Incident was supposed to be material risk that should not have been overlooked, but it was excluded from the list of material risks at the field-level judgement without adequate examination at the top management.

(2) Inadequate management after selecting material risks

After selecting material risks, the Risk Management Committee confirmed the overall control methods and the direction, and then issued instructions to perform quarterly review of the quantity of risks related to each division and report the results. However, the Committee did not provide any opportunity to discuss activities to deal with risks allocated to each division.

2. Ineffective risk management resulting from personal risk judgement

In GMO-PG, Chairman of the Risk Management Committee serves concurrently as Chairman of the Information Security Committee and General Manager of the System Division, which has created an environment where it is difficult to properly manage risks through double-checking from various viewpoints.

Also, GMO-PG has a corporate culture that highly values individual ability and gives certain discretion and authority to make decisions. While it can accelerate decision-making at the field-level, it is also possible that a judgment error by a field staff at an initial stage could eventually lead to serious management risk.

Moreover, the risk management rules allow to establish subcommittees in order to monitor and control individually material risks. However, because roles and responsibilities were not clear among the Risk Management Committee, the System Division, and the Information Security Committee, the matrix-type checking function was not working as planned.

3. Slowdown of educational and awareness activities

It is possible that the Company focused largely on risks that directly affect immediate company interest such as the shortage of system development power or risks of delay in delivery or service starting date, and neglected educational and awareness activities in long-term perspective. Consequently, responses to the Company’s various and constant risks may have been insufficient.

VII. Recurrence Prevention Measures

Based on the reported matters described from II to VI above, the Recurrence Prevention Committee decided to implement the recurrence prevention measures as listed below.

Description of technical recurrence prevention measures are kept to the minimal as it may become a security risk.

1. Technical prevention measures

(1) Short-term measures

(a) Improvement of measures to block unauthorized request (entry control measures)

(b) Improvement of measures to prevent placement of malicious program

(c) Improvement of data cover-up measures (no data retention by masking important data, etc.)

(d) Improvement of measures to prevent data from being taken out (exit control measures)

(2) Medium-term and long-term measures

(a) Abolition of existing Struts 2

The alternative framework will be selected by comparing risk factors (e.g. number of vulnerability in the past) and support availability.

(b) Improvement of unauthorized access detection at SQL-level

(c) Performance of re-audit of PCI DSS for the entire system of GMO-PG

2. Prevention measures related to information security management

(1) Securing human resources in the security group

The security group should recruit personnel with expertise in information security. And then, by utilizing the expertise of such personnel and taking into consideration of opinions of risk management personnel and compliance personnel, the security group should review the entire information security management including system development and operation, as well as revise internal rules and review operation.

(2) Risk assessment

(a) Participation of external specialists

The Information Security Committee should have someone with expertise in information security (preferably external specialist) among its members so that the Committee can check the completeness of the risk items for risk assessment and perform risk assessment effectively such as verifying reasonableness of assessment of asset value, threats and vulnerability.

(b) Clarification of the roles of the Information Security Committee

The internal rules and the organization structure must be reviewed in order to clarify allocation of roles in risk assessment between the Risk Management Committee and the Information Security Committee and actions to be taken by each committee.

For example, the Information Security Committee may be placed under the Risk Management Committee, and the Information Security Committee would perform system-related risk assessment and report to the Risk Management Committee.

(3) Reconsideration of procedures for security incident reporting

(a) Promptly obtain vulnerability information

In order to improve the methods of obtaining vulnerability information, a system to share vulnerability information with relevant parties within the company utilizing various information sources should be established.

(b) Develop information escalation process related to vulnerability information

It is necessary to clarify an information escalation process by updating manuals for the escalation process including checklist, flowchart, and contact lists. It also must be ensured that relevant personnel of both the Information Security Committee and the System Division can share information.

(4) System development

(a) Clarify software selection criteria

GMO-PG should clarify the criteria to select software used in system development by considering the following factors: what type of vulnerability has been detected and how often, how long it would take from the announcement of vulnerability to the release of security patches, and whether system security support for the software from external service providers is available. If software assessed as inappropriate under this selection criteria is used in the existing systems, suspension of the use of the software should be considered promptly.

(b) Further crystallize the security-related internal rules

GMO-PG should clarify the system security standard and the system development standardization standard in order to further crystallize the security standard to be followed in each process of system development such as requirement definition, design, constructing and testing.

(c) Deepen cooperation between the security group and the development group

On the premise that the security group better understands security of individual systems based on its enhanced authority and increased resources as described in (1), the security group and the development group should share their security issues (issues related to individual systems' security, in particular). And then, both group should closely cooperate in order to assess those issues and discuss and implement specific measures to solve them.

(5) Educational activities related to information security

GMO-PG should revise training materials or arrange trainings by external instructors in order to provide employees with opportunities to gain knowledge about serious threats, detection of unauthorized activities, and other methods of attacks.

3. Prevention measures related to corporate risk governance and corporate culture

(1) Issues related to enterprise risk management

(a) Measures for process to identify risks and select material risks

It is desirable that assessment of individual risks should be performed by all members above certain managerial position, rather than by limited personnel of the responsible department. It is also important for selection of material risks to establish a control method based on the internal control's vulnerability assessment criteria.

Based on the above vulnerability assessment, the residual risk of individual risks should be evaluated and the relevant risk control measures should be decided.

(b) Measures against inadequate management after selecting material risks

The current risk management rules stipulate that the Risk Management Committee meeting shall be held more than once a year, but from a perspective of PDCA, it should be held at least on a quarterly basis and the status of significant risk management should be confirmed.

(2) Measures against increasing risks under the system managed by a few responsible personnel

Leaving the judgment of risks affecting the entire company to a certain on-field employees involves substantial and excessive risks. Accordingly, reporting to and approval from the board of directors or a director in charge should be required during the process of such decision making.

(3) Measures against slowdown of educational and awareness activities

Many issues that require improvement were identified as a result of the Incident. Measures to solve these issues include many technical measures such as system improvements, but most personal and organizational improvement will be achieved mainly through educational and awareness activities. It is important to plan educational and awareness activities as yearly events, not as a transient measure, so as to prevent these incidents from recurring and manage these improvement activities to take root in the organization.

4. Implementation of recurrence prevention measures

GMO-PG implemented the following prevention measures by April 14, 2017, based on the recurrence prevention measures of 1, 2, and 3 above decided at the Recurrence Prevention Committee.

- Short-term technical prevention measures
- Reconsideration of procedures for security incident reporting
- Revision of guidelines regarding system development process

In addition, as efforts to relaunch the Metropolitan Tax Payment Site and to prevent recurrence, the Company conducted PCI DSS assessment by PCF on the Metropolitan Tax Payment Site and the Insurance Rider Payment Site. As a result, it was confirmed that they satisfy the PCI DSS requirements as of April 14, 2017.