Yoshiharu Ueki, Representative Director & President, Japan Airlines Co., Ltd.,

Verification Report

(Summary)

January 14, 2015

Verification Committee of Independent Executives

Concerning the Theft of Customer Information

Chapter 1 Background and Objective of the Establishment of the Verification Committee of Independent Executives Concerning the Theft of Customer Information

Section 1: Background of Establishment

Because slow responses occurred in the Customer Information Management System (hereinafter "VIPS") of Japan Airlines Co., Ltd. (hereinafter the "Company") on September 19 and 22, 2014, an emergency internal investigation was conducted. As a result, JAL confirmed evidence of a security incident (hereinafter the "Event"), in which malware[1] which had infiltrated internal business computers with access to VIPS (hereinafter "VIPS computers") communicated with VIPS, stole personal information of certain JAL Mileage Bank (hereinafter "JMB") members, and sent it to an outside server in Hong Kong (hereinafter "a Hong Kong server").

On September 24, two days after the Event was discovered on September 22, the Company began consultations with the Metropolitan Police Department, submitted a report to the Ministry of Land, Infrastructure, Transport and Tourism, and set up an internal investigation framework centering on IT Planning and Loyalty Marketing. With the assistance of specialized security vendors with advanced IT security technology, the Company started investigations to identify the cause, define the scope of damage, and establish preventive measures and take other corrective action (hereinafter "primary investigations"). Additionally, at the regular press conference on September 29, 2014, the Company disclosed facts that they had learned up to that time and announced their policy to disclose necessary information at times in accordance with the progress of the investigations.

In the course of the primary investigations, it was discovered that there was the possibility that a malicious third party infiltrated several internal business computers by some means prior to September 19, 2014 and stole personal files stored in those computers. Accordingly, investigations were conducted to verify personal files stored in those business computers, analyze communication records and other data, and identify the possibility of theft and the scope of the damage (hereinafter "secondary investigations").

Primary and secondary internal investigations were conducted immediately after the discovery of the Event through the middle of November, and ultimately, IT Planning submitted a report to the Board of Directors at its meeting held on November 21, 2014.

Meanwhile, to verify from an objective perspective whether the details, scope, and method of the internal investigations were appropriate and whether the countermeasures and other corrective action to be implemented were appropriate, the Board of Directors decided at its meeting held on October 29 to establish a Verification Committee of Independent Executives Concerning the Theft of Customer Information (hereinafter the "Verification Committee") comprised of independent outside executives. Commissioned by the President, the Verification Committee was set up on October 31, 2014.

The Verification Committee was set up because the Event was a serious problem affecting public trust in the Company and because it was determined that verification of internal investigations by a committee composed of independent outside executives would ensure the transparency of the internal investigations and would be effective in guaranteeing the fairness and independence thereof. Furthermore, a Verification Working Group was placed under the Verification Committee and, to ensure expertise in carrying out verifications, the verification work thereof was entrusted to outside IT consultants.

Section 2: Objective of Establishment

The Verification Committee was established for the following objectives and to submit the results of verification to the President.

<1> Verify whether the details, scope, method, and other aspects of the primary investigations were appropriate

<2> Verify whether the details, scope, method, and other aspects of the secondary investigations were appropriate

[1] A general term for a program, such as a virus, that acts maliciously.

<3> Verify corrective action with respect to the theft of personal information leaked from VIPS, and recommend new corrective action as necessary

<4> Provide findings and recommendations on improvement concerning problems in customer information management by the Company in general, which were discovered in the process of verifications noted in <1> and <2> above.

Chapter 2 Members of the Verification Committee

The Verification Committee was comprised of five independent executives of the Company. A Secretariat and Verification Working Group were set up under the Verification Committee to render support.

Section 1: Members of the Verification Committee

Chairman (elected by the committee from among its members)	Kimie Iwata, Japan Airlines Co., Ltd. External Director
Member	Tatsuo Kainaka, Japan Airlines Co., Ltd. External Director
Member	Eiji Katayama, Japan Airlines Co., Ltd. External Audit & Supervisory Board Member
Member	Hiroyuki Kumasaka, Japan Airlines Co., Ltd. External Audit & Supervisory Board Member
Member	Shinji Hatta, Japan Airlines Co., Ltd. External Audit & Supervisory Board Member

Section 2: Secretariat
Japan Airlines Co., Ltd., General Affairs

Section 3: Verification Working Group
Deloitte Tohmatsu Financial Advisory Co., Ltd. (hereinafter "DTFA")

Chapter 3 Method of Verification, etc.

Section 1: Scope of Verification
The Verification Committee established the scope of verification below and verified the validity of each item.

<1> Verification of responses to and internal investigations of the Event

- Appropriateness of the initial response
- Appropriateness of the investigation policy
- Appropriateness of the investigative structure

<2> Verification of investigation by specialized security vendors

- Appropriateness of investigations by JPCERT Coordination Center (hereinafter "JPCERT")
- Appropriateness of investigations by NRI Secure Technologies (hereinafter "NRI")
- Appropriateness of investigations by S&J Consulting (hereinafter "S&J")
- Appropriateness of the McAfee investigations

<3> Verification of the primary investigations

- Appropriateness of investigations of the route of malware infection
- Appropriateness of investigations of theft of personal information
- Appropriateness of investigations of the cause

<4> Verification of the secondary investigations

- Validity of the policy of investigations to identify the scope of impact on business computers not directly related to the theft of personal information
- Validity of investigations to identify the scope of impact

<5> Verification of security measures prior to the Event

<6> Verification of emergency measures and issues to be addressed

- Appropriateness of emergency measures
- Appropriateness of issues to be addressed
- Recommendations regarding preventive measures and corrective action

<7> Recommendations regarding measures with respect to customers whose information was confirmed to have been stolen.

Section 2: Verification Method and Period

The Verification Committee held eight meetings as noted below, and received reports from the Verification Working Group engaged in verification and from the Secretariat. The members held discussions, created a mailing list among themselves, shared information and exchanged comments as necessary, and compiled this report.

	Date	Main Topic of Discussion
1st Meeting of Verification Committee	October 31, 2014	- Confirm direction of verification - Interviewing and verification of reports on internal investigations
2nd Meeting of Verification Committee	November 12, 2014	- Interviewing and verification of reports on internal investigations
3rd Meeting of Verification Committee	November 19, 2014	- Interviewing and verification of reports on internal investigations
4th Meeting of Verification Committee	November 26, 2014	- Interviewing and verification of reports on internal investigations
5th Meeting of Verification Committee	December 10, 2014	- Interviewing and verification of reports on internal investigations - Sort issues
6th Meeting of Verification Committee	December 17, 2014	- Consider preventive measures - Confirm policy of composition of Verification Report
7th Meeting of Verification Committee	December 24, 2014	- Consider Verification Report
8th Meeting of Verification Committee	January 7, 2015	- Finalize Verification Report
Submission of the Report	January 14, 2015	

Section 3: Verification Work by the Verification Working Group

The Verification Committee chose DTFA as the Verification Working Group to which the verification work was entrusted. DTFA was chosen because of its adequate knowledge and experience in collection and analysis of IT-related data, IT security measures, and risk management in general.

The Verification Working Group carried the following work at the request of the Verification Committee.

<1> Conduct interviews of IT Planning, Loyalty Marketing, etc., which were in charge of internal investigations

<2> Conduct several interviews of four specialized security vendors who assisted with internal investigations and JAL INFOTEC (hereinafter "JIT") which assisted with initial action, and verify necessary data submitted by each of these companies

<3> Tabulate and summarize results of verification, and report to the Verification Committee

Chapter 4 Results of Verification of Internal Investigations

Section 1: Overview of Results of Internal Investigations

In this section, we will provide an overview of the Report of Results of Internal Investigations prepared by IT Planning and Management, which was the subject of verification by the Verification Committee.

<1> Background and cause of the Event

- Slow responses of VIPS occurred on September 19 and 22. In the course of IT Planning and Management investigating the cause, it was discovered that the cause was unauthorized access by malware that had infiltrated VIPS computers.
- Furthermore, as evidence of communication over the Internet by some of these VIPS computers with a Hong Kong server was confirmed and as customer information was downloaded from VIPS by a method not normally adopted during usual operations and stored in these VIPS computers, IT Planning and Management determined that there was a high possibility of the theft of customer information.
- Furthermore, in addition to the Event, IT Planning and Management determined there was the possibility that personal information stored in business computers infected by malware had been viewed by a malicious third party.

<2> Overview of damage by the theft of personal information

[Result of primary investigations]

As a result of the investigations, it was determined that certain personal information of 4,131 customers had been stolen by extracting data from VIPS and sending it to a Hong Kong server. It cannot be determined whether credit card information was included in that data.

[Result of secondary investigations]

It cannot be determined whether any personal information stored on individual business computers subject to these investigations was stolen.

<3> Emergency measures

With the assistance of specialized security vendors, IT Planning and Management implemented the following measures as emergency measures.

- Prevent the spread of malware infection by restricting connections to dangerous sites
- Add a request for authentication when accessing external sites from all internal business computers
- Prevent theft of information through a new function to detect malware

<4> Preventive measures and issues

In addition to emergency measures, IT Planning and Management determined it necessary to implement the following measures and heighten security.

- Heighten security authentication over the Company's website
- Remove malware from all internal business computers
- Introduce a framework to detect malware attached to e-mails
- Improve IT Security Education for JAL staff and JAL Group company staff

Section 2: Overview of Results of Verification

In this section, we will provide an overview of the results of verification by the Verification Committee concerning the results of internal investigations.

<1> Verification of basic responses to the Event

Investigations of the Event were conducted on the assumption that two different types of routes were used through which personal information was improperly accessed.

- Primary investigations: The possibility that customer data was stolen from VIPS computers and sent to outside parties using an unauthorized program
- Secondary investigations: The possibility that files stored in business computers infected by malware were viewed by or sent to outside parties

In the primary investigations, business computers that had communications with outside parties that could not have occurred in normal work were identified from past communication records. A calculation was made of the volume of communication noted in communication records and the volume of data that could have been sent based on the transmission data/time. We feel that this method of investigation was reasonable since it logically covered routes through which internal information was sent to outside parties over the network and since it confirmed evidence of all information that had been transmitted.

In the secondary investigations, the subject of the investigations was specified in accordance with the following criteria, and investigations were conducted.

- Business computers confirmed to have communicated with a Hong Kong server
- Business computers confirmed to have been accessed without authorization using administrator authority of the Company’s network
- Business computers s confirmed to have evidence of installation of known malware or unauthorized timers etc.

To conduct investigations of the Event, specialized security vendors were entrusted with work in processes requiring high expertise, and advanced knowledge and operation. Considering the urgency, making this investigation request was inevitable. Investigations consigned by the Company were conducted by each vendor in accordance with the Company’s request. As vital information was provided by the vendors, we feel that both the method and results of investigations were appropriate.

<2> Validity of internal investigations

[Primary investigations]

Detailed investigations were conducted of 20 business computers having the possibility of having had communications with a Hong Kong server through malware. As a result, the computers which had sent customer information to outside parties were narrowed down to three. It was also confirmed that the malware that had infected the computers was compressed to the “.rar” format using compression software “RAR” for sending information to outside parties. Accordingly, investigations were conducted of these three computers. If the size of the compressed file in the “.rar” format and the size of the transmitted file as noted in transmission records matched, this would be judged as evidence of theft of customer information.

As a result, a history of transmission matching the size of a “.rar” file assumed to be made by malware was discovered. As information of 4,131 customers had been stored in the file, it was determined that data of 4,131 customers had been sent to a Hong Kong server.

As the size of the file and transmission records matched and information was sent immediately after the “.rar” file was created, we feel that the judgments of these investigations are appropriate.

[Secondary investigations]
Files were narrowed down by file name extension[2] and the contents of all files were visually scrutinized on business computers possibly infected by malware and possibly processing personal information. On business computers without the possibility of processing customer information, files were narrowed down by file name extension and then checked as to whether they contained customer information using a checking tool. Files containing even one image data and customer information were further scrutinized. As a result of the investigation of transmission records of all business computers, evidence of the theft of personal information stored on these computers was not confirmed.
As identification of files and investigations using transmission records were conducted, as in the primary investigations, we feel the results of these investigations are appropriate.

Chapter 5 Verification of Security Measures prior to Discovery of the Event

Prior to the discovery of the Event, the Company had implemented security measures such as, but not limited to, the following.

- Auditing of systems in compliance with J-SOX
- Establishment of various manuals such as Information Security Manual and JMB Personal Information Manual
- Regular auditing of work according to the above manuals
- Installation of a proxy server in Internet connection areas
- Installation of malware preventive software in business computers
- Information security training for JAL staff and JAL Group company staff
- Advisory agreements with several specialized security vendors

As no flaws in these security measures were found and they appear appropriate, we conclude that appropriate measures had been implemented in advance.
However, because these security measures did not stop this theft of certain information, the company will consider additional preventive measures.
Regarding this point, improvement has already been seen as a result of continued usage of certain systems that were introduced as part of the emergency measures in response to the Event. Additionally, manuals on handling customer information have been continually updated, however there is no evidence that these updates would have prevented the Event.

Chapter 6 Verification of Emergency Measures and Issues to be Addressed

Points requiring quick consideration were verified, such as, but not limited to, the issues of human resources not subject to system auditing, daily work and handling of information, and peripheral systems and the network from the perspective of “the Company’s network and systems composing the network.”

<1> Staff awareness promotion activities and review of the information management system

- Prepare training material using the Event as a case study which actually happened in JAL, and review the ideal IT security training for JAL staff and JAL Group company staff
- Review the customer information management policy so as to refrain from storing customer information in personal business computers as much as possible from the viewpoint of work efficiency
- In addition to personal information, identify data corresponding to sensitive information in the Company’s

[2] A suffix to a computer file name to distinguish the type of file

business and redefine the sensitivity level, and build an information management framework and operation according to the sensitivity level.

<2> Develop a sophisticated framework with respect to cyber incidents

- Establish an internal Security Operation Center (SOC) function, and aim to manage and operate information over the system (Security Information and Event Management (SIEM))
- Taking into account the possibility of another cyber incident, gather information on specialized security vendors in advance to prepare for unified responses in case of a contingency

<3> Review the internal network and systems

- Control virtualization[3] of the connection environment and connection to devices containing sensitive information, and restrict unauthorized access to the Company's sensitive information from both inside and outside the Company's network
- Rebuild the system to manage account authority
- Reconsider the physical layout[4] and logical layout[5] of the network, such as by subdividing the internal IP network or establishing space dedicated for handling sensitive information

<4> Adoption of a neutral verification function

- Consider establishing a function to make neutral decisions on the validity of the purpose of introducing systems and software, such as specs, scope and cost effectiveness

Chapter 7 Measures for Customers Whose Information was Confirmed to Have Been Stolen

We feel that actions by JAL Public Relations regarding the Event, uploading of messages over the Company's website, and other response actions were speedy, and that notifications and actions were appropriate.
Though actual damage/loss has not been reported at the moment, we recommended that the Company should respond sincerely in cases in which customers suffer some kind of loss.

Chapter 8 Summary

We feel that initial response of investigations into the Event, notification to related organizations, actions by JAL Public Relations, prevention of the spread of malware infection, and actions to respond to the Event based on the results of investigations were conducted speedily, and that responses to the Event based on the method and the results of investigations were appropriate.
However, cyber-attack techniques by malicious third parties have become extremely sophisticated, and technical measures for systems and networks alone will not completely prevent cyber-attacks. Therefore, it is important to establish and implement security measures that strike a balance between "hard" measures for systems and networks, etc. and "soft" measures for human resources and work/operation, and we look forward to further improvements.

End

[3] Technology to cause computer resources such as computers, storage devices, networks etc. to appear and operate differently from the actual physical configuration

[4] A configuration made by physically connecting devices and cables

[5] A configuration partitioned by, for example, restricting functions of software or connections in a system or a network, that is different from the physical configuration