November 4, 2016

For Immediate Release

Shinsei Bank, Limited
Shinsei Investment & Finance Limited

Notice Regarding the Possible Leakage of Information Due to a Malware Infection of a PC Terminal in Shinsei Investment & Finance, a Member of the Shinsei Bank Group

It has come to the attention of the Bank that the computer terminal of an employee in Shinsei Investment & Finance Limited (Chiyoda-ku Tokyo; President and Representative Director Masanao Taniya; hereinafter "SIF"), a Group member company of Shinsei Bank, Limited (Chuo-ku, Tokyo; Representative Director and President Hideyuki Kudo; hereinafter "Shinsei Bank" or the "Bank") was infected by a malicious program (malware) and that there is a possibility of a leakage of corporate and personal information of the obligors of claims held by YMS9 Yugen Kaisha (special purpose company or *Tokutei Mokuteki Kaisha* (TMK); hereinafter, "YMS9"), a subsidiary of SIF.
The following paragraphs describe the details of this incident and any actions which have or will be taken in order to rectify this matter.

The Bank extends its sincerest apologies for any concerns and inconveniences this incident may cause our customers and other concerned parties. Due to the serious nature of this incident Shinsei Bank and SIF will engage in efforts to further enhance information security management structures of the Shinsei Bank Group in order to prevent the recurrence of any similar incidents.

1. Overview and background

(1) Nature of Relationship between Shinsei Bank and SIF

SIF is a wholly-owned subsidiary of Shinsei Principal Investments Limited, a wholly-owned subsidiary of Shinsei Bank, and engages in investment and lending operations.
Shinsei Bank provides some of its Group member companies including SIF with the use of Bank's network infrastructures and oversees the monitoring and operation of cyber security.

(2) Development of this incident

On Tuesday, October 25, 2016, Shinsei Bank's cyber security system detected that an SIF employee's personal computer terminal downloaded a suspicious file (malware) from an external site through a "phishing e-mail." In response to this detection, the Bank isolated this terminal from the network on the same day, took measures to remove the suspicious file including scanning the terminal with security software, and following the completion of such measures reconnected the terminal to the Bank's network."

On Thursday, October 27, Shinsei Bank's cyber security system detected that this terminal was transmitting data to a specific external site on the Internet. On the same day, Shinsei Bank once again isolated the terminal from the network again discovered that screenshots of the browser of this terminal had been periodically taken and automatically transmitted to an external malicious site on a regular basis from Tuesday, October 25 to Thursday, October 27.

The analysis of the infected computer terminal conducted on Thursday, October 27 revealed that i) obligor information of 35 claims held by YMS9, ii) information on a claim transfer agreement, and iii) information described in two mail or other delivery certificates may have been leaked between the dates of Tuesday, October 25 and Thursday, October 27 during which the automatic transmission to the malicious site occurred. Such information had been handled by two internal information systems accessed by the personal computer terminal. The Bank has also determined that the failure of the security software utilized in scanning the affected terminal in detecting the malware was due to the malware being previously unknown.

Following the report from SIF, Shinsei Bank reported the details of this incident to its supervisory authorities. The Bank has so far not confirmed any unlawful use of information that might have been leaked in this incident. In addition, no access by other computer terminals to the external malicious site detected in this incident has been detected in the networks of Shinsei Bank or its Group member companies, which are controlled by the Bank.

2. Information that may have been leaked

(1) Obligors' information on 35 claims

SIF is entrusted by YMS9 with administrative operations for claims held by YMS9. Information on 35 claims held by YMS9 includes obligors' trade or personal names, the status of claims, repayments made and their collection schedule. Of the 35 claims, 27 include information of individuals.

(2) One agreement for the assignment of claims

Information on an agreement for the assignment of claims between YMS9 and a corporate customer includes the name and address of this corporate customer, its representative's name, the name of a joint guarantor (an individual) of the claims.

(3) Two mail and other delivery certificates

The trade names and representative's names of corporate customers described in mail and other delivery certificates dispatched by YMS9.

3. Responses to customers who might be affected by this incident

Since November 2, 2016, SIF has been contacting corporate and individual customers whose information may have been leaked in order to provide a full explanation of the situation. SIF is asking customers to contact them in the event they suffer any damage due to the misuse of leaked information. SIF will continue to provide support to its customers in relation to this incident.

4. Recurrence prevention measures

Shinsei Bank and SIF are fully aware of the gravity of this incident. In order to prevent the recurrence of any similar incidents, we will therefore promote the transfer from the fat-client terminals to thin-client terminals as a measure to strengthen information security for Shinsei Bank and its Group member companies whose networks are controlled by the Bank; revise and enhance security measures and the method of implementing them; and further improve employees' training and education.

End