September 10, 2014

Report and Response Regarding Leakage of Customers' Personal Information

Recently, a former employee of an outsourcing contractor to Synform Co., Ltd., a Group company that carries out systems development and operations for Benesse Corporation (hereinafter "the Company") transferred important personal information of the Company's customers externally without authorization, and sold the information to a name list provider. Once again, we tender our deepest apologies for the concern and inconvenience this incident has caused.

The Company has cooperated fully with a police investigation since the matter came to light, and has implemented emergency measures to ensure the safety of its databases and taken action to prevent the leakage of customers' personal information from spreading. Moreover, on July 15, we established a Personal Information Leakage Incident Investigation Committee, chaired by Mr. Hideaki Kobayashi, an attorney, and the committee has been working to conduct a thorough investigation of the facts of the incident and to uncover the cause with external experts and create measures to prevent a recurrence.
Today, we hereby report on the facts that have been revealed to date by the reports from the internal investigation and the abovementioned investigation committee, as well as on the Company's response.
The Company will continue to make every effort to prevent damage to customers, and to work sincerely to recover customer trust by taking swift measures to prevent a recurrence. Details of the report are as follows.

1. Number of Customers Whose Personal Information Was Leaked and Content Thereof

It has been revealed that the former employee of the outsourcing contractor acquired customers' personal information without authorization, and sold 35.04 million items of information to three name list providers.
However, it is believed that this number is greater than the number of those affected, and the actual number is estimated to be about 28.95 million.
The content of the information leaked to the name list providers is as follows.

- Name, gender, and birthday of the registrant for a service
- Names, genders, birthdays, and relationship of parents or children who were registered together with the registrant

- Zip code
- Address
- Telephone number
- Fax number
- Expected birth date (only customers using certain services)
- Email address (only customers using certain services)

No evidence whatsoever has been found to indicate that credit card information was sold to the name list providers.

2. Course of Events and Cause of the Unauthorized External Transfer

The investigation revealed that despite the external systems and audits that have been in place, the system was not prepared for criminal action by a malicious insider. As a result, there were several security holes that allowed the criminal activity to occur. In light of findings from the incident investigation, we have determined that the basic issue for the Company was an overly lax approach. This was due to a company culture characterized by overconfidence in in-house information security functions, insufficient IT literacy, including among management, and audits and a supervision structure that assumed human nature to be fundamentally benign.

Regarding the specific course of events, the former employee of the outsourcing contractor was engaged to perform database maintenance and management at Synform Co., Ltd. In order to perform his duties, he was granted access privileges to the database that was transferred externally without authorization. He used these privileges to extract the customers' personal information onto a work computer and then transferred it externally without authorization using his personal smartphone. The following facts have been uncovered as reasons why this unauthorized action was not prevented.

(1) Restriction on Writing Data to an External Memory Device

Internal regulations prohibit the writing of data held in a work computer to an external media device, and in operation, a system was in place to control such activity. However, when this system was being updated to a newer version, the system was operated with the write-control function not supporting writing to certain smartphone models. The former employee of an outsourcing contractor to the Company exploited this weakness to write data to his personal smartphone.

(2) Alert Setting of the Database that was Transferred Externally

The internal network environment of the Company has an alert function set up to sound an alert when a large volume of data is handled. However, the alert function setting did not include the database from which the customers' personal information was externally transferred.

(3) Checks of Database Access Logs

The system automatically creates an access log whenever someone accesses the database from which the customers' personal information was transferred using a work computer. However, these logs themselves were not regularly monitored and checked. We recognize that if we had a sufficient checking function to perform regular monitoring, the unauthorized action in this case might have been detected at an early stage.

3. Measures to Prevent Recurrence

We have taken the results of this investigation seriously and have formulated the following measures to prevent recurrence. These measures are currently in effect.

1) Emergency Measures for System Security and System Operation

Flaws in the system security were a direct cause of the incident. Following the incident, we engaged one of Japan's largest information security specialist companies, LAC Co., Ltd., to conduct an audit with respect to these flaws, and we have now implemented the following emergency measures. These measures are now in effect for all Benesse Corporation databases that contain personal information, including the database involved in the leak.

Emergency Measures

(1) Access privileges reviewed and granted only to the absolute minimum number of people necessary. Password management has been strengthened.

(2) Supervisor established to oversee downloads to terminals.

(3) Alert function set up to operate when a large quantity of data is downloaded.

(4) Measures implemented to prohibit connection to external recording media on work terminals.

(5) Access log monitoring setting strengthened (regular checks)

(6) Ban instituted on bringing personal electronic devices and recording media into operation spaces, and security cameras installed.

2) Reform of Overall Group Information Management System and Organization

To significantly increase security levels, we will reform the structure of our organization model and strengthen the Group's IT governance. We will now separate the following three functions for our data systems and clarify authority and responsibility.

(1) Database Management: Benesse Holdings, Inc.

Database management will be performed by Benesse Holdings, specifically monitoring and auditing of data security management, and supervision, and operational status.

The framework is as follows. A corporate senior vice president will be established as a Chief Legal Officer (CLO) with responsibility for internal control and audits, including of information management. The CLO is scheduled to be appointed in October, and will be a person with a strong background as a specialist in a global organization. Moreover, under the CLO will be established the Chief Information Security Officer (CISO), with responsibility for information security audits, and the Database Management Division, which will perform database management.

(2) Database Maintenance and Operation: Joint Venture

A joint venture will be established to handle database maintenance and operation, which was highlighted as an issue in the recent incident.

Establishment of Joint Venture

Benesse Holdings has concluded a basic agreement with the information security company LAC Co., Ltd. on establishing a joint venture. We are now aiming to build one of the most highly secure maintenance and operation frameworks in the world. Following the establishment of the new company, we will integrate the necessary assets and human resources from Synform Co., Ltd., which has undertaken operation and maintenance until now, into the new joint venture.

(3) Database Usage: Group Company

Group companies will use the databases for planning and provision of products and services, as well as marketing activities and so forth. However, in doing so they will follow the guidelines set out by the abovementioned Database Management Division, separate database management and maintenance and operation, and ensure that they uphold customers' confidence.

Moreover, the activities of the entities in items (2) and (3) above will be monitored and audited by Benesse Holdings as noted in item (1).

3) New Establishment of External Monitoring Organization
Furthermore, we will establish an external monitoring organization, which will perform regular audits on all Group data and system management, maintenance and operation from an independent perspective. The external monitoring organization will include external leading members of experience and academic standing with knowledge of information security and personal information. Their duty will be to conduct rigorous audits and deliver fair judgments from the customers' perspective.

4) Outsourcing of Database Management and Operation
Database maintenance and operation will now be performed by the newly established joint venture, based on the above security measures. Our policy is to cease outsourcing these operations to providers outside the Group.

4. Initiatives to Prevent Damage to Customers

On August 4, we established the Customer Headquarters to serve as a dedicated customer support unit.
We are taking steps to prevent damage to Benesse Corporation customers. Based on information received from customers and our independent investigation results, we are identifying operators that are highly likely to be using the leaked information. We are also taking steps to stop operators from using the information after confirming that they are highly likely to be doing so. We are also making every effort to prevent the leakage of customers' personal information from spreading by cooperating with the police and public institutions.

5. Communication with Customers and Apology

We will send letters of apology and reports in stages to customers whose personal information is confirmed to have been leaked to the three name list providers. Since a very large number of customers have been affected, we do not expect to finish notifying all customers until late October. Again, we apologize for the length of time taken to contact everybody.
Furthermore, as a token of apology from the Company to customers who have been inconvenienced by this incident, we will prepare a 500 yen gift voucher (e-money gift card or a book voucher that can be redeemed throughout Japan).

6. Establishment of the Benesse Children's Fund Foundation

We recognize that this incident has resulted in a very serious situation, and that the leak has affected an enormous number of people throughout Japan, causing widespread inconvenience. The Company is deeply conscious of its responsibility to society for this situation, and as further gesture of apology, the Company will use part of a 20 billion yen fund to establish a foundation called the Benesse Children's Fund.

The Benesse Children's Fund will work to support children, who represent the future and to secure an environment where children can approach learning with peace of mind, among other objectives. We will form a Board of Directors comprising external experts such as persons involved in government and educational specialists and continue to examine ways to support and contribute to children so that they will be ready to lead in the future.

Examples of Foundation Activities and Assistance

- Support learning and higher education for children struggling with financial difficulty or sickness
- Provide learning support for children to prepare then to live in a global society (e.g. international exchange, support for overseas study, etc.)
- Act to protect children's safety and security
(e.g. Promotion of activities for children regarding crime prevention and social initiatives relating to protection of personal information, etc.)
- Other activities related to supporting the development of children

Moreover, customers who choose to do so can donate the abovementioned apology gift voucher (or e-money gift card) of 500 yen to the Benesse Children's Fund, rather than receive it themselves. If customers choose to do this, we will donate 500 yen to the fund instead, to assist with the foundation's activities.

7. Impact on Business Results

The impact on the consolidated business results of Benesse Holdings, Inc. is currently being examined.

We plan to announce the impact on the forecast results for the fiscal year ending March 31, 2015 in our second quarter consolidated financial results.