

July 2, 2009

Mitsubishi UFJ Securities Co., Ltd.

To whom it may concern:

Submission of business improvement report to FSA

Responding to the business improvement order and the recommendation regarding the incident of the customer information leak dated June 25, 2009, we submitted the business improvement report to FSA today and it was accepted.

We are committed to carrying out the preventative measures written in this report, and have also imposed punishments on relevant employees impartially in order to clarify their responsibilities for the incident of the customer information leak.

The summary of the business improvement report is as per enclosure.

While fully cooperating with the police investigation, we will continuously put all our efforts into preventing further damages to our customers and regaining their confidence and trust by quickly implementing the measures necessary to prevent recurrence of such an incident.

July 2, 2009

Summary of Business Improvement Plan

Fumiyuki Akikusa
President & CEO
Mitsubishi UFJ Securities Co., Ltd.

The recent information leak by our former employee has undermined the trust of the public toward the financial industry. It is highly regrettable that an employee who should have protected customer information actually leaked the information. We take this incident very seriously and would like to sincerely apologize to our clients and all who were affected by the incident.

Customer information forms the basis of trades of financial instruments and their intermediary services. It is very important to manage such information from the perspective of personal information protection, and we dedicate ourselves to regaining the customers' trust by carrying out the above mentioned drastic preventative measures.

We will continuously put all our efforts into implementation of the business improvement measures, regarding the benefit of our precious customers who have suffered excessively from this incident as our top priority.

I. Actions necessary to protect affected customers and limit damages to customers

(1) Internal actions

We established an emergency headquarters and issued a news release titled "Customer Information Leak Incident yet to be Identified" on March 30, 2009, because we had been getting inquiries from customers who were receiving unsolicited calls from real-estate agents and other companies, and we suspected a leak of our customer information. We also set up a "Contact Center" for this incident.

Subsequent investigation found that our customer information had been leaked, and we held a press conference on April 8.

On April 14, in order to respond to this incident, we established a special task force named "Task Force on Customer Information Leak" (hereinafter called the "Task Force") led by President and CEO, Fumiyuki Akikusa. We announced the establishment of the Task Force on April 17.

On April 21, with the aim of clarifying processes for investigation and evaluation, we established an independent investigation committee consisting of Lawyer Takashi Ejiri (the head of the committee), Lawyer Tadashi Kunihiro and Professor Norihisa Doi. The committee investigated facts and causes of the incident and prepared an “Investigation Report” including their opinions from a standpoint of an outsider. The committee submitted the report to the head of the Task Force on May 15.

(2) Actions for customers

1) Apologizing and notification to customers whose information was leaked

Our staff called or visited around 50,000 customers whose information had been leaked, to notify them of the incident and make a sincere apology to them.

In addition, we sent a letter of apology on April 9 and a letter on our incident-related actions from May 8 through May 15 to each of the affected customers.

2) Establishment of a contact center and a special page on our website

To answer customers’ consultations and inquiries, we established a contact center for this information leak incident on March 30, which commenced operation on March 31.

We also added a special page to our website on April 30 to show how we are tackling this incident.

In addition, we posted “examples of customer inquiries relating to unsolicited calls” as well as some advice on countermeasures against these relentless solicitations, and provided a link to the website of the National Consumer Affairs Center of Japan on our website on June 11.

(3) Requests to data brokers and solicitors

1) Delivery of warning letters to data brokers and solicitors to call on them to cease and desist utilizing our customer information list

To the brokers and solicitors to whom we found our customer information had been leaked, our attorneys issued warning letters to call on them to cease and desist using the list of our customer information for solicitation, and not to resell or use the list for any purpose. We are also collecting the list from identified brokers and solicitors, and ensuring that they pledge not to manipulate or utilize the list in the future.

2) Measures against relentless solicitation

Our attorneys, acting as agent for the customers who delegated the issue to our attorneys, have warned the solicitors to stop unsolicited calls immediately. We asked each of customers to

forward all the calls from solicitors to our attorneys in the future.

3) Legal actions against brokers and solicitors

If the above actions do not stop the solicitors from making unsolicited calls, we are seeking a temporary injunction forbidding them from using the list of our customer information.

(4) Delivery of “Sincere Apology Gifts”

Taking into account the significance of this incident, financial and mental damages to the customers and our social responsibilities, in late June, we delivered gift cards worth 10,000 yen as “Sincere Apology Gifts” to customers whose information was leaked.

(5) Future actions

We are determined to keep the contact center open to support customers, give top priority to customers and make our best efforts to implement the above measures including request to solicitors not to use our customer information, delivery of warning letters, and legal actions against unprincipled solicitors.

We will announce our incident-related actions on a timely basis on our website.

II. Clarification of the responsibility of relevant staff including senior management

To highlight the significance of this incident, and the fact that it has caused immense harm to our customers, we have clarified the responsibility for the incident, and imposed internal disciplinary actions to relevant staff including President & CEO according to the internal rules, for safeguarding the integrity of information security controls.

III. Preventative measures

(1) Improvement to governance framework

Taking this event and the committee’s recommendations seriously, we will commit ourselves to improving the governance framework for the oversight of secure effective risk management.

1) Reinforcement of approach to System Risk

We regard to the “Operating Risk and Information Security Committee¹”, it is the place to discuss measures based on risk assessment (or to enforce risk-based approaches). In the committee, we will strengthen the commitment of the senior management to the information security, and develop more effective and rational risk management.

¹ Operating Risk and Information Security Committee is established as an advisory body for risk management meetings equivalent to the Board of Directors according to “Information Asset Risk Management Rules.”

2) Enhancement of the information security governance

To unify the control functions of information security, on July 1, we transferred the information system security control functions which had been governed by the IT Strategy Division to the Information Securities Management Division. This makes it possible to enhance the monitoring and check-and-balance function over system related divisions.

3) Enhancement of the audit function toward system related divisions

While reviewing the audit program with regard to the information security which Systems Audit Office of Internal Audit Division has, we will make efforts to improve our audit skills to enhance the depth of internal auditing.

(2) Expansion and enhancement of information security management framework

1) Proper check-and-balance function among divisions

Along with the above enhancement (1)-2), we reorganized IT Strategy Division on July 1, and segregate the functions of system development, operation and monitoring, and clarified the surveillance framework for system related divisions.

2) Verification and effectiveness of the actual operations relating to security control procedures including outsourced operations

We have a policy for appropriate protection of personal information called “Policy of the Protection of Personal Information”, and basic rules for information security called “Information Asset Risk Management Rules.” In addition, we also set forth the “Procedures for Information Management”, “Procedures for the Protection for Personal Information” and “Procedures for Information System management.”

However, the policy and rules had not been strictly followed in the Operator Room, and they also have room for improvement.

Therefore, to verify and ensure the effectiveness of the actual operations relating to security control procedures including outsourced operations, we have set forth operating management rules and manuals exclusively for the Operator Room and keep all the staff informed of the contents of the rules and manuals.

3) Review of procedures for management of access authorities of relevant employees, identification of weaknesses which could allow fraudulent use of sensitive information, and de-concentration and segregation of such authorities to strengthen the control-and-check system for those employees

The tort-feasor has been engaged in development and operation of search tools for customer information and similar data. However, the access authorities which could allow fraudulent use of private customer information were not segregated and also the control-and-check system for relevant employees was not sufficient.

Therefore, in order to improve the weaknesses, we have divided and restructured the IT Strategy Division into the IT Planning Division and IT Development & Service Division on July 1, and also newly created the IT Service Office within the IT Development & Service Division as an independent operational department with an aim to de-concentrate the authorities related to development and operation of such systems.

Additionally, we have improved the frameworks to administer IDs and passwords, and to monitor log data for search and access to customer information, and enhanced the preventive function by installing more monitoring cameras.

4) Other measures necessary for the prevention of fraudulent cover-up activity

The tort-feasor has used an ID of another employee in order to cover up his fraudulent activities. It was possible because access authorities of users were not terminated properly. Therefore, we have strengthened the control-and-check function to terminate access authorities. We have also strengthened the supervision of the log-data of such systems which can be used to search customer information.

(3) Improvement of the human resources management

1) Educational training related to the code of ethics and other important awareness

The top management will send all the employees the messages indicating the determined attitude toward the fraudulent clearly, in any possible opportunities. We will also improve the awareness of the employees in order for all employees to acknowledge the code of ethics thoroughly.

2) Implementation of educational training for management

We will implement educational training for management covering a wide range of areas such as personnel management and observation of employees' behavior.

3) Implementation of educational training for all the employees

We will implement appropriate educational trainings adapting the characteristics of each division based on the unified theme of "prevention of fraudulent activities".

4) Education and training for the employees working at IT divisions

We will implement appropriate education and trainings suitable for IT related divisions.

5) Implementation of educational training for the staff doing outsourced jobs

We will implement educational trainings similar to those for IT related divisions, for the staff doing outsourced jobs, regarding the code of ethics and information security regularly (semi-annually).

(4) Review of information security control and others

1) Strengthening of the audit of Systems Audit Office of Internal Audit Division toward the IT related divisions

We will give more effort to acquire and improve the system audit skills by re-examining the audit program of Systems Audit Office related to the information security and adding experts of external audit to the team for the actual audit of divisions.

2) Implementation of monitoring measures to prevent recurrence

- Information Security Management Division will review the effectiveness of preventative measures and report the progress to the executive committee monthly until September and quarterly thereafter.
- Internal Audit Division and Systems Audit Office will audit the above mentioned process during the second half of this fiscal year.
- We will get an audit from a third party regarding the administrative framework for the information security by the end of March next year.

EOD