Investigation Report

May 20, 2011

Special Investigating Committee on System Failures

I. Outline of Investigation

1. Background to Establishment of Committee

Over the period between the night of March 14, 2011 to the 24th of the same month, Mizuho Bank, Ltd. (hereinafter referred to as "MHBK") experienced massive information system failures (hereinafter referred to as "Failures"). During this period, the customers' economic activities were seriously affected by delays in payroll remittances and other fund transfers as well as outages of ATMs, among other problems.

MHBK decided to investigate into the causes of the Failures and develop measures to prevent the recurrence of similar events. Given the scale of the impact of the Failures on customers and society, it has determined to work to prevent the recurrence of the information system failures and recover the public trust by establishing a third-party committee comprising outside experts and specialists and having it investigate the causes of the Failures, assess the adequacy of, and make recommendations regarding the recurrence prevention measures from a neutral and impartial viewpoint. On this basis, MHBK requested several legal professionals and systems specialists who do not have a vested interest in MHBK to become members of the committee, and on April 11, established the Special Investigating Committee on System Failures (hereinafter referred to as "Committee").

2. Constitution of Committee

Chairman	Tatsuo Kainaka (Attorney-at-law, former justice of the Supreme Court)
Member	Masahito Monguchi (Attorney-at-law, former President of the Nagoya High Court)
Member	Yoriko Goto (Certified public accountant, Managing Partner, Financial Services Industry Group, Deloitte Touche Tohmatsu LLC)
Member	Yasumasa Takeda, Executive Vice President, Accenture Japan Ltd.

The Committee appointed the following parties as assistants to help the Committee with its investigation:

Assistants to the Investigating Committee

Anderson Mori & Tomotsune

Deloitte Touche Tohmatsu LLC

Accenture Japan Ltd.

3. Purpose of Investigation

The purpose of the investigation by the Committee is to (i) identify the causes of the

information system failures and to (ii) assess the adequacy of, and make recommendations regarding MHBK's recurrence prevention measures.

The Committee's purpose is nothing but to investigate into the above-mentioned matters from an independent and fair position to prevent the recurrence of the information system failures. It is not that the Committee aims to determine whether or not each individual involved in the Failures is legally or managerially liable and to pursue their responsibilities.

II. Method and Scope of Investigation

The Committee examined and analyzed MHBK's internal data gathered upon and after the Failures, the systems audit reports, the relevant rules and regulations concerning system operations, the contracts with outsourcees and other materials, and conducted a total of forty-seven (47) hearings of MHBK's President, Directors, Officers and employees as well as the representatives of Mizuho Financial Group, Inc., the Mizuho Group's holding company (hereinafter referred to as "MHFG"), representatives of Mizuho Information & Research Institute, Inc. (hereinafter referred to as "MHIR") and Mizuho Operation Service, Ltd. (hereinafter referred to as "MHOS"), which are MHBK's outsourcees, and other related parties, as necessary.

The Committee limited the investigation to the period up to April 11, 2011 for the impact and scope of the Failures, and to the period up to April 30, 2011 for the actions taken by MHBK after the Failures, with the main aim of conducting a prompt and precise investigation in view of the nature of the matters for investigation by the Committee and the gravity of the Failures.

III. Facts Detected as a Result of the Investigation

1. Summary of the Failures

(1) Summary of the Failures

The Failures subject to this investigation stemmed from the abnormal end of the Core Banking System on Monday, March 14, 2011 (unless otherwise stipulated, the year indicated herein refers to the calendar year of 2011) because the volume of processing of the Night Batch of the Core Banking System exceeded the Limit Value as a result of concentrated transfers and remittances to certain donation accounts in the wake of the Great East Japan Earthquake which took place on Friday, March 11.

Although MHBK took measures to restore the system to solve the above-mentioned abnormal end of the Night Batch, MHBK took many hours to do so and it became highly likely that the sequence of the Night Batch would not terminate by the open time of its business offices on Tuesday, March 15. For this reason, MHBK elected to suspend the

Night Batch and launched the Business Office Terminals, and conducted operations to inhibit such transactions as it would be unavailable due to the possible impact of the Night Batch it had suspended.

However, it took time to complete those operations and MHBK was delayed in opening its business offices on Tuesday, March 15. Furthermore, MHBK could not terminate the Night Batch it had suspended on the same day because the system operations that should have been normally automated were switched to manual operations due to the daily processing of the batch (hereinafter referred to as the "DJS Switching") necessary to launch the Business Office Terminals, and also could not send exchange transactions which it was supposed to process after the Night Batch was terminated.

In the morning of Wednesday, March 16, MHBK terminated the Night Batch for Monday, March 14 and started the Night Batch for Tuesday, March 15. However, there was the same concentration of remittance and transfer processing operations as occurred on Monday, March 14 for a different account from the donation account that suffered the system trouble on Monday, March 14, and the Night Batch abnormally ended in the early morning of Wednesday, May 16. After that, the open time of the business office operations was delayed on Wednesday, March 16, because MHBK had to conduct operations to inhibit transactions as it did on the previous day and respond to the ATM failures. Subsequently, the number of unprocessed operations of the Night Batch increased and there were many human errors arising out of the manual operations of the system, as a result of which the extent of influence became wider and wider.

In order to secure system resources and prevent unsent exchange transactions from increasing, MHBK imposed ATMs and Direct Channel usage restrictions and conducted stagnant operations of the Night Batch during the period of Friday, March 18 to Tuesday, March 22 including the three consecutive holidays. However, the Night Batch subsequently remained unprocessed due to shortage of processing time and human errors. Moreover, the Failures triggered many additional events which affected customers, such as the unavailability of the certain transaction details.

(2) Categorization by the Event that Caused the Failures

The events that caused the Failures were categorized into: (i) delays in processing the exchange transactions; (ii) delays of the open time of the business offices and suspension of transactions; (iii) ATM outage and usage restrictions; (iv) Direct Channel usage restrictions; and (v) other events that affected customers. See Attachment B: "Conceptual Diagram of MHBK System and Points of System Failures Occurred."

2. Outline of the System

The current Core Banking System was based on the systems that the former The Dai-Ichi Kangyo Bank, Ltd. (hereinafter referred to as "DKB") had started to operate in 1988, and restarted to run in tandem with the systems of the former The Fuji Bank, Ltd. (hereinafter referred to as "FBK") at the time of the management consolidation with FBK in 2002. After connecting those systems by a temporary system through relay computers, MHBK migrated and consolidated the former FBK systems into the former DKB systems between July and December 2004. The current status of the MHBK systems including the consolidated Core Banking System is as described below.

(1) Summary of the Current MHBK System

The current system consists of various kinds of systems to offer a variety of services, including, among other systems, the Core Banking System to execute exchange and other transactions in which MHBK receives and pays deposits through the ATMs and its business office counters, and sends and receives data to and from other financial institutions via the Zengin System (Japan Bankers Association's Data Telecommunications System); the External Connection System (Customer) that accepts transaction requests from and provides information to the ATMs, business offices and other customer channels; the Information Support System that analyzes and provides data and information; and the Securities/Market System.

(2) Summary of the Core Banking System

The Core Banking System is called STEPS, which manages the ledgers based on "customer attributes," "deposit and exchange transactions," "lending and foreign exchange transactions," "securities (JGBs)" and other transactions and processes deposit/settlement transactions. The processing operations through STEPS are largely divided into the online operations instantly processed and the Night Batch processed in bulk. In STEPS, MHBK expected the daytime online operations and the Night Batch to be processed alternatively, and it was not designed such that the both operations would be done at the same time.

The Core Banking System of Mizuho Corporate Bank, Ltd. (hereinafter referred to "MHCB"), a member of the Mizuho Financial Group is a separate system from MHBK's system. However, in processing the certain funds transfer transactions, it processes data in tandem with the MHBK Core Banking System, unlike the systems of other financial groups.

The following describes the chronological process of STEPS operations at MHBK:

- 8:00 Business Office Terminals launched, online operations started
- 15:30 Transmissions via the Zengin System closed
- 16:30 Sending of exchange transactions between the head office and branch offices closed
- 17:00 Business Office Terminals closed, online operations ended
- From 18:00 to early morning Night Batch (continued to the next day)
- 4:30 DJS Switching
  Due at 6:00 if the Night Batch is delayed

For clarity, the ATMs and Direct Channel operate 24 hours a day during the above-mentioned processing.

The Night Batch is managed by the automated operation system called TARGET. TARGET automatically runs nearly 30,000 individual data processing features (hereinafter referred to as the "Batch Jobs") a night, takes over data created when they are run, and manages magnetic tapes and other media. The Limit Values of the Night Batch of STEPS were fixed for each of 40 blocks consisting of MHBK's head office and branches across Japan.

The DJS Switching is a process to create the Batch Jobs for the next day and is run after all of the Batch Jobs on the current day are completed. Such processing is regularly scheduled to be run at 4:30 or, in case of a delay of the Night Batch, 6:00. If, however, MHBK could not complete the Night Batch by 6:00 and launch the Business Office Terminals (hereinafter referred to as the "Night Batch Processing Delays"), it was supposed to conduct the DJS Switching, in which case there would have been no choice but to delay the online operations start time, including a delay of transaction start time in the branch offices, or to suspend the Night Batches and start online operations on schedule. If, however, MHDK elected to suspend the Night Batches and conduct the DJS Switching, it was structured such that MHDK would execute the remaining parts of the Night Batch manually and could not send exchange transactions until it terminated such Night Batch

Therefore, in case of the Night Batch Processing Delays, STEPS latently encompassed a threat of the system failures occurring, such as a delay in the transaction start in the business offices or a delay in sending exchange transactions.

(3) Summary of the Next-generation System

Discussions about the next-generation system were started chiefly principally by MHFG in 2004 to rebuild the enlarged and complicated current system as new system in an attempt to address the rapid changes in the business environment.

In the initial "Next-Generation IT Systems Basic Plan" published in 2004, they aimed to complete the first step and the second step in FY2005 and FY2006, respectively, and complete the third step by the end of FY2011 under the investment plan. However, the second step was completed in FY2010 and it is now in the third step, which has not yet been completed.

(4) Contracts with the Related Organizations and Contractors for the System Development and Operations

A. MHBK's System Development/Operations Structure

At MHBK, the IT & System Division is responsible for system development and management, project supervision and management, IT strategies, IT-related investments, and next-generation system construction, while the System Operation Division is responsible for system management and system center management and administration.

The IT & System Division oversees MHIR, a MHFG's subsidiary, with which it contracts to provide system development services, while the System Operation Division oversees MHOS, with which it contracts for system operation and system center management and administration.

The IT & System Division conducts in evaluating and checking MHIR's status of system development (such as determination of role allocation, determination of an deployment release, and inspection of process-completed products), plays the responsible roles of effectively administering the system limit management, and checks with MHIR, among others, the relevance and points of issue of its analysis, and its coping policies.

On the other hand, MHIR is responsible for the sequence of system development, such as designs, program creation and system testing, under various regulations and rules.

The System Usage Department within MHBK (hereinafter referred to as the "User Department") checks definitions of the business requirements, user acceptance tests, user training, education and migration rehearsal programs, from a users' viewpoint.

B. Roles of the Related Organizations for System Development/Operations

MHBK has entered into a Master Contract for Outsourcing with MHIR for STEPS system development, which provides that the regulations and rules to be complied with by MHIR shall be separately expressly stipulated after discussion, as necessary. Under this agreement, the memoranda (oboegaki) for the regulations and rules to be complied with by MHIR have been separately concluded.

The System Operations Department has entered into the Master Contract for Outsourcing with MHOS for STEPS system operations, and has designated the details of

services outsourced with MHOS, business management, persons conducting the businesses, and other relevant matters under the relevant Individual Engagement for Outsourcing.

C. Information Technology Risk Management-related Organs and Their Roles

Within MHBK, the IT Strategy Committee must make necessary deliberations and adjustments in order to conduct appropriate Information Technology Risk management based on the location, size and attributes of the Information Technology Risk inherent in the business operations. The executives in charge of the IT System Group must oversee any matters relating to the planning and operations of the Information Technology Risk management and take necessary measures. The IT & System Division is responsible for the Information Technology Risk management planning and promotion.

D. System Audit-related Organs and Their Roles

Within MHBK, the Operations Audit Department is responsible for the IT and system-related internal audit, and conducts internal audit under the master audit plans for each fiscal year, with the aim of verifying the effectiveness and appropriateness of the Information Technology Risk management, and has external audit, as necessary. The Operations Audit Department of MHBK conducts audits of MHIR and MHOS under the relevant external audit contracts.

Within MHIR, its Operations Audit Department conducts organization/theme based internal audits. Alternatively, the Operations Audit Department of MHFG presents the basic policy for the group-wide audit functions to the internal audit departments of each of the companies within the MHFG Group, and request each of them to make reports on the audit results. Each company establishes its audit plans based on the risk assessments, conducts system audit, and makes reports on the results of such audit to MHFG.

E. Emergency Responses

The Procedures for System Contingency Plan designates the role sharing rules to respond to failures and troubles, under which MHIR must locate the causes, draw out failure response plans and inform them to the IT & System Division, and then the IT & System Division or the executive in charge must determine failure response policy. However, the chain of command for both MHBK and MHIR is not necessarily clear.

(5) Various Rules Concerning the Failures

MHBK has rules which are divided into the Articles of Incorporation, etc., the Organization Related Rules, the Business Continuity Management Related Rules, the

Business Operations Related Rules, and the Human Resources Related Rules. The Business Continuity Management Related Rules, among other rules, stipulate the basic policies, structures, roles, contingency plans and other relevant matters in case of emergency.

A. Business Continuity Management Related Rules

The Business Continuity Management Related Rules are categorized into the following areas: basic policies in case of emergency; structures and roles in case of emergency; guidelines for development and administration of contingency plan; procedures for system contingency plan; business contingency plan and procedures; and drills under the Business Continuity Management Related Rules.

(a) Rules Stipulating the Basic Policies in Case of Emergency

The rules stipulating the basic policies in case of emergency consist of: the Basic Policies on Business Continuity Management, the Detailed Rules for the Basic Policies on Business Continuity Management, and the Guidelines for Business Continuity Management.

The Basic Policies on Business Continuity Management defines the patterns that should be assumed as emergency (17 common patterns for the MHFG Group), matters to be prepared in anticipation of emergency, and the bank-wide emergency structures (Emergency Headquarters/System and System Emergency PT (hereinafter referred to as the "Response PT"). The Detailed Rules for the Basic Policies on Business Continuity Management defines the scope of the Group companies to which the Basic Policies on Business Continuity Management are applicable; magnitude of each company within the Group; and matters each company within the Group is required to report. The Guidelines for Business Continuity Management defines the methods for analysis and assessment of business exposures, the obligation to establish a contingency plan based on the business exposures, and the roles of the Response PT.

(b) Rules Stipulating the Emergency Structures and Roles

The rules stipulating the emergency structures and roles consist of the following subordinate rules of the Guidelines for Business Continuity Management: the Emergency Response Manual and the Action Plans for Emergency Response (for each emergency situation).

The Emergency Response Manual defines the structures and roles for each

Response PT, while the Action Plans for Emergency Response (for each emergency situation) defines the common rules for all organizations, such as the interdivisional information coordination flow and roles for each division.

(c) Rules Stipulating the Guidelines for Development and Management of Contingency Plan

The rules stipulating the guidelines for development and management of contingency plans consist of the following subordinate rules of the Emergency Response Manual: the Procedures for System Contingency Plan and the Manual for the Development of Contingency Plans (for each business process).

The Procedures for System Contingency Plan defines the unit of and guidelines for development of the system contingency plan, as well as the maintenance rules for those plans, substantiate the contents of the System Department's Emergency Response Manual, and designate the ultimate decision-makers and other officials within each organization.

The Manual for the Development of Contingency Plans (for each business process) defines the unit of and guidelines for development of the business contingency plans, as well as the maintenance rules for those plans.

(d) Rules for System Contingency Plan and Procedures

The rules for System Contingency Plan consist of the Procedures for System Contingency Plan and its subordinate rules entitled "Contingency Plan for Individual System" and "System Contingency Plan (for each emergency scenario)."

The Contingency Plan for Individual System has been developed at each system unit level by assuming the times of disaster and failure, and depicts each system's configuration diagram, correspondence system and chain of command at the time of disaster or failure, system restoration patterns based on the conditions of operation, and the titles of the related steps, procedures and other processes. That plan also consists of the System Recovery Manual which includes the recovery procedures at the time of failure, and has the subordinate rules of the Basic Policies on Information Technology Risk Management entitled "Procedures on Switch over to the On-Site Backup System," which defines the procedures on switching to the backup system at the time of disaster.

The System Contingency Plan (for each emergency scenario) has been developed at the center unit level on the assumption that the center would suffer disaster, and depicts, among others, the related system configuration diagrams and

restoration time charts.

(e) Rules for Business Contingency Plans and Procedures

The rules for business contingency plans include the Business Contingency Plans (for each business process) under the Manual for the Development of Contingency Plans (for each business process), and define the responsible organizations and teams, operation names, assessment of business exposures, related systems, target restoration time and other relevant matters. The rules relating to the business contingency plans consist of the Business Operations Procedures in Emergency Situations, which define the specific business operations procedures when the Business Contingency Plans (for each business process) are implemented.

(f) Rules for Drills under the Business Continuity Management Related Rules

The rules for drills under the System Contingency Plan consist of the Guidelines for Recovery Drills of System Failures, under which annual drill plans have been drawn out and there is at least one drill a year for most significant systems and significant systems.

With respect to the business contingency plan drills, the annual drill plans have been drawn out for the business contingency plan designated each year pursuant to the Business Continuity Management Related Rules, under which MHBK is supposed to conduct each department-level and bank-wide (once a year) drills.

B. Other Business Operation Related Rules

(a) Procedures for Inspection of System Limit Value

In connection with inspection of system Limit Value, hardware, software, program-related resources and capacity alarm value, and threshold limit value, among others, are controlled pursuant to the Guidelines for System Capacity Management (IT Department System) in order to avoid computer system faults and processing capacity slowdown, and MHBK must verify its ability analysis and status of use based on the cycle of such management.

(6) Emergency Framework

MHBK's emergency framework is such that the President & CEO oversees business continuity management and, when an emergency situation occurs, the President & CEO, on his own judgment, establishes the "Emergency Headquarters" led by himself or the "Emergency Response PT" led by his designee based on reports made by each of

responsible executives, all pursuant to the Basic Policies on Business Continuity Management (hereinafter referred to as the "Basic Policies") prescribed by the Board of Directors, to gather information, determine what response policy to adopt, and give response and other instructions.

The Basic Policies define the "emergent situations" resulting from the system failures as "when it becomes difficult to conduct business due to any computer hardware or software malfunction, and any system failures attributable to operation error or otherwise, or when any event is threatened to have a material effect on the evaluation of the MHBK Group." If this is the case, the IT & System Division is required to make a report to the President & CEO via the executive in charge of the IT/System Group pursuant to the Reporting Standards for System Failures developed by the IT & System Division.

The above-mentioned Reporting Standards for System Failures categorize a system failure, when it occurs, into five ranks based on the extent of impact (on management, external/internal, or intra-IT Department affairs, and degree of impact (number of customers affected, number of transactions affected or duration of time affected) and, as for system failures in the top three ranks that should have any external impact, requests the IT & System Division to make prompt reports, via the executive in charge of the IT/System Group, on the assumed maximum extent of impact, availability of alternative means, expected restoration time, and other relevant aspects.

Furthermore, if any system failure that requires any emergent response such as suspension of settlement functions occurs, the Action Plans for Emergency Response (for each emergency situation), which defines the coordination and reporting flows between the responsible departments and to the management team based on each of the emergency situations, requests the executive in charge of the IT/System Group to inform and report on the status of system operations, status of business operations, and status of the business offices to the President & CEO.

3. System Failures Which Had Occurred Prior to the Failures, and Responses

MHBK consistently took the following responsive measures to improve its systems based on previous system failures, including the large-scale failures resulting from the system integration which had occurred in April 2002.

(1) System Failures Which Had Occurred after the System Integration in April 2002, and Responses

On Monday, April 1, 2002, MHBK and MHCB experienced account funds transfer processing delays and settlement and other system failures as a result of the system

integration (hereinafter referred to as the "2002 Large-scale Failures"). MHBK experienced significant effects on its customers because of account funds transfer processing delays, double debits, transfer delays, and restrictions on ATM transactions. In that case, as the causes for the failures which had occurred at MHBK, the causes and recurrence prevention measures published by the MHFG (formerly Mizuho Holding ("MHHD")) referred to the fact that MHBK had not conducted sufficient system tests and had not been prepared even at the minimum level required" and that the checking system had not worked sufficiently because of critical problems with the reporting and correspondence lines within the Group," and explained that it was basically caused by the fact that the old management team had not fully recognized the risks resulting from the system integration, which had led to delays in decisions of basic matters such as the system development effort associated with the system integration, and they could not secure sufficient duration of time necessary for system development, system tests and clerk training.

In response, MHBK developed recurrence prevention measures mainly intended for reinforcement of the management structure of the system project that had immediately caused the 2002 Large-scale Failures, and also developed a total of 30 measures to create a new corporate culture for the recovery of confidence, including the establishment of a code of conduct based on the lessons from the Large-scale Failures and inauguration of the new structure resulting from the management consolidation. All of these measures had been put into practice with the completion of the system integration in December 2004.

As for the system failures which had occurred in and after 2002, the IT & System Division identified the causes for those failures, investigated into their consequences, and drew out the restoration measures in cooperation with the System Operation Division, development vendors, and operation vendors, and then implemented the restoration efforts, which were summarized in a System Failures Report after the restoration.

(2) Implementations of the System Audit

A. Implementations of the Internal Audit within MHBK

With respect to internal audit, the recurrence prevention measures for the 2002 Large-scale Failures provides that MHBK should improve its internal audit structures in an attempt to enhance the methodology and content of audits (including, among others, utilization of external audit).

In the case of internal audit, the basic audit plan for each fiscal year is developed pursuant to the Internal Audit Practice Guidelines. In the "Review of Risk Assessment Structure and Result of Assessment" issued in February 2010, the risk assessment of

"system operation management" that is highly related to the system failures that occurred recently was rated "MH"[1] (i.e., a field that highly requires audit and in which audit should generally be conducted) which is lower by one notch than the highest level, and the risk assessment of "deposit/exchange system features" was rated "R2"[2] (i.e., a field in which audit is to be conducted within 30 months). Accordingly, internal audit was conducted pursuant to the IT Audit Procedure. The results of the risk assessment were ranked the same as in FY2009.

B. Utilization of External Audit

The Operation Audit Department utilized external audits for the internal audit of the system integration project as the "Integration Project Audit (planning phase)" in 2003, and as "Advisory for the Integration Project Audit (migration phase)" in 2004. The Information Technology Risk Management Office of IT/System Department was subject to external audits in 2005, 2006 and 2007. There has been no external audit of that office since 2008.

C. Conduct of System Audits at MHIR and MHFG

At MHIR, the system audit of STEPS in which the Failures had occurred was to be audited by MHBK, the system owner and it was not subject to system audit by the Internal Audit Department of MHIR.

At MHFG, there is the framework in which MHFG can exercise the right to audit directly, as well as the right to make reports, under the Basic Policy of Internal Audit established by MHFG. However, MHFG had not directly audited NHBK or MHIR prior to the Failures.

4. Fact that the Failures Occurred

(1) What Occurred and Restoration Measures

A. Exchange Processing Delays

There were substantial delays in exchange processing between Tuesday, March 15 and Thursday, March 24. The background to the occurrence of such exchange processing delays is described below:

---

[1] The Guidelines for Assessment/Monitoring of Risk categorize the fields for each purpose of control into the following 4 ranks: H, MH, ML and L (in descending order of risk). The highest category "H" includes, among other items, "information security management (related to systems)" (as of August 2010).

[2] The Guidelines for Assessment/Monitoring of Risk categorize the fields for each organization/system feature into the following 4 ranks: R1, R2, R3 and R4 (in descending order of risk). The highest category "R1" includes, among others, "lending and foreign exchange system features" (as of August 2010).

(a) Incomplete Inquiries into Deposits and Transaction Details

After the Great East Japan Earthquake which occurred on Friday, March 11, there was an immense volume of transfers to Company A's donation account <a>. As a result of this immense volume of transfers, the number of transaction details exceeded the Limit Value of online inquiries which was the default of the underlying system at 10:16 on Monday, March 14, which made it impossible to utilize the "inquiry into deposits and transaction details" function for the donation account <a> through the use of the Business Office Terminals.

MHBK requested Company A to open a new "REEF" (see Note below) corporate donation account which requires no passbook and switch instructions as to the donation account to the new account, and finished opening the new account at 11:30 on Monday, March 14.

(Note) The attributes of the account can be chosen from "individual" or "corporate," and "REEF account" or "passbook account." A feature of the REEF account is that it requires no passbook. The account attributes of the above-mentioned donation account <a> required passbook and was an "individual/passbook account" which had a lower system processing Limit Value when the Failures occurred. When the above-mentioned donation account (a) was opened with the Tokyo Chuo Branch in September 2005, it was the "individual/REEF account" and was changed to the "individual/passbook account" at the request of Company A that wanted to know the transfer details in December 2007. The above-mentioned donation account <a> was also used as the donation account for the Great Sichuan Earthquake in April 2008 after it was changed to the "individual/passbook account." There was no failure at that time.

(b) Abnormal End of the Night Batch and Extended Operations (Monday, March 14)

Many transfer requests to the donation account <a> in which MHBK could not completely respond to inquiries into deposits and transaction details as explained in subsection (a) above the continued, and the amount of processing of these transfers exceeded the Limit Value of the number of processing per account in the Night Batch (see Note below), and the Night Batch abnormally ended at 22:07 on Monday, March 14. Some of the processing result data was also lost when it abnormally ended.

(Note) Generally, to process credits based on the transfer requests accepted after 15:00 in the Night Batch, MHBK temporarily evacuates the transaction details already processed during the online hours on the current day, and processes credit of the amounts transferred after 15:00. On Monday, March 14, MHBK implemented the Night Batch in this procedure. However, the Night Batch abnormally ended as explained above, because the number of transfer requests exceeded the Limit Value of the number that MHBK could process when it evacuated the processed transaction details.

After the above-mentioned abnormal end of the Night Batch, MHBK took restoration measures to raise the Limit Value that caused it and rerun the Night Batch. However, the subsequent processing needed the processing result data which was lost when the above-mentioned abnormal end occurred. MHBK faced difficulty in this data restoration effort. It eventually took nearly 8 hours to finish, extending the duration of the Night Batch.

(c) Suspension of the Night Batch and Manual Operation (Monday, March 14)

The duration of the Night Batch for Monday, March 14 was extended as explained above, resulting in a shortage of time for preparations for launching the Business Office Terminals after the termination of the Night Batch, and led to concerns about a delay in the transaction start time utilizing the Business Office Terminals. In response, MHBK suspended the Night Batch at or around 7:00 on Tuesday, March 15 pursuant to the applicable procedure document[3] to launch the Business Office Terminals on the scheduled time, and started preparing for launching the Business Office Terminals and implementing the DJS Switching.

Although the Night Batch was normally designed to plan and run batch jobs by automated operation, it became impossible to utilize such automated operation as a result of the suspension and implementation of the DJS Switching. For this reason, MHBK had to run the Night Batch manually until the underlying system was normalized. As a result, a tremendous volume of work was generated, triggering many secondary failures due to failed processing and misprocessing.

(d) Abnormal End of the Night Batch and Extended Operations (Tuesday, March 15)

As a result of Company B starting to call for donation through the use of mobile

[3] Online Response in Night Batch Processing Delays.

phone-based transfer service[4] on Tuesday, March 15, an immense volume of transfers were made to the donation account <b> after 15:00 on Tuesday, March 15. Although the person in charge of such service within MHBK checked the data volume it could accept through EBIS, the number of transfers exceeded the Limit Value of the number of processing per account in the Night Batch on Tuesday, March 15, as a result of which the underlying system abnormally ended at 7:17 on Wednesday, March 16.

Because the error message that appeared when the Night Batch for Tuesday, March 15 abnormally ended was similar to the message to the Night Batch of the donation account <a> for Monday, March 14, MHBK took measures to increase the Limit Value based on the restoration method it adopted on the previous day and reran the Night Batch. However, as the similar abnormal end occurred after the rerun, MHBK reran it again after taking measures to further increase the Limit Value four times between 19:20 on Wednesday, March 16 and 4:13, Thursday, March 17. Despite this effort, the abnormal end was not solved. Then, MHBK determined that it was caused by the donation account <b>, and reran it after temporarily removing such data. MHBK finished the Night Batch other than that of the donation account <b> data at 5:20 on Thursday, March 17.

At 13:30 on Thursday, March 17, MHBK erased the unnecessary data which was inhibited due to the automated operation of the Night Batch after evacuating the necessary data. However, MHBK learned that it had lost the necessary data in the course of the subsequent work. In order to respond to this, it took 5 hours to identify the data lost, and 11 hours to recreate such data, which led to a further delay in the duration of the Night Batch.

Finally, the Night Batch for Tuesday, March 15 ended at 19:05 on Saturday, March 19.

(e) Suspension of the Night Batch and Automated Operation (Tuesday, March 15)

Although MHBK tried to launch the Business Office Terminals after ending the Night Batch for Tuesday, March 15, the abnormal end of the Night Batch described in subsection (d) above occurred at 7:17 on Wednesday, March 16. As it took time to restore it, MHBK suspended the Night Batch and decided to launch operations of the Branch Office Terminals. So, MHBK started to prepare for launching operation of

[4] The service that enables customers to remit money by designating the mobile phone number of the recipient.

the Branch Office Terminals and implement the necessary DJS Switching.

(f) Unsent "SHIMUKE" (Outbound Instruction) Exchange Transactions

As a result of the above-mentioned suspension of the Night Batch for Monday, March 14, the "SHIMUKE" (Outbound Instruction) exchange transactions which were scheduled to be run on Tuesday, March 15 after the end of the Night Batch were left unsent.

During that period of time, each of the branch offices conducted the "transmission of the transfer data for which processing had not been withdrawn" (release operation; hereinafter referred to as the "Release Ope") and made transfers by separate "DAKEN" (input) of remaining unsent data. However, the processing which should have been completed prior to the Release Ope did not meet the Zengin deadline, and no exchange transmission through the Release Ope was made. On the other hand, only the exchanges processed by the separate "DAKEN" (input) were sent, because the transmissions by the separate "DAKEN" (input) were made independently from the Night Batch. As a result, approximately 310,000 exchange transactions which should have been sent on Tuesday, March 15 were left unsent at around 17:00 on Tuesday, March 15.

With respect to those unsent exchange transactions which should have been sent on Tuesday, March 15, MHBK expected to send them together with the transactions which it should have sent on Wednesday, March 16. However, the Night Batch for Tuesday, March 15 was left suspended as explained above, and the exchange transactions which should have been sent on Wednesday, March 16 were also left unsent. Furthermore, the continuation of the extended operations of the Night Batch eventually left parts of the customer requests for exchange transaction on Thursday, March 17; Friday, March 18; and Tuesday, March 22, and Wednesday, March 23 unsent (approximately 1,200,000 transactions in total).

Because only parts of the exchange transactions were sent by the separate "DAKEN" (input), the sent exchange transactions might have been sent doubly had those unsent exchange transactions been sent in bulk. For this reason, MHBK needed to cancel the inputs already made.

(g) Unprocessed "HISHIMUKE" (Inbound Instruction) Exchange Transactions

As a result of the extended operations of the Night Batch, the other banks' requests for exchange transactions for the periods between Wednesday, March 16 and Friday, March 18 (a total of approximately 1,010,000) were let unprocessed.

(h) Recovery Response to the Exchange Processing Failures

As the extended operations of the Night Batch was not solved until Thursday, March 17, MHBK decided to secure its system resources by imposing restrictions on usage of ATMs, Direct Channel and other services between Friday, March 18 and Tuesday, March 22, including the three consecutive holidays, and put the greatest emphasis on solving unsent exchange transactions, and solving the extended operations of the Night Batch on and after Tuesday, March 15 which left the exchange transmissions unsent.

In order to make the manually processed Night Batch more efficient, MHBK automated its processing by improving the TARGET. Although there was no schedule for parallel operations of daytime online and the Night Batch in STEPS, MHBK started considering the technical aspects of such parallel operation on Monday (holiday), March 21, and successfully identified them. Then, MHBK decided to automatically operate its daytime online and the Night Batch in parallel on Tuesday, March 22. As a result, MHBK could finish the Over Time Batch for up to Monday, March 21 during the duration of the daytime online operations on Tuesday, March 22, and the Night Batch for Tuesday, March 22 after which it was switched to the normal automated operation.

As a result, the majority of the unsent “HISHIMUKE” (inbound instructions) exchange transactions were solved on or prior to Tuesday, March 22. However, on Tuesday, March 22, some of those transactions (nearly 160,000) were left unsent, and on Wednesday, March 23, parts of those transactions (nearly 1,000) were also left unsent for the same reason, which was solved on Thursday, March 24.

In order to secure the convenience of customers in connection with the restrictions on usage of ATMs, Direct Channel and other services, MHBK temporarily launched its Business Office counters between 9:00 and 17:00 on the holidays from Saturday, March 19 to Monday, March 21 (holiday), and made special payments (i.e., payments of up to ¥100,000 only based on any personal identification document, without checking the ledger balance).

B. Delay in the Open Time and Suspension of the Business Office Operations

As a result of the abnormal end of the Night Batch for Monday, March 14 and the abnormal end of the Night Batch for Tuesday, March 15 as explained above, there were the delays in the business office open time and suspension of the business office operations, as described below..

(a) Delay in the Business Office Open Time and Suspension of the Business Office Operations

At around 7:00 on Tuesday, March 15, it became impossible for MHBK to provide lending, loan, foreign exchange and other services due to the suspension of the Night Batch for Monday, March 14, which forced MHBK into implementing nearly 100 transaction inhibition operations. Although the time necessary for the work of the above-mentioned transaction inhibition operations was initially estimated at about 30 minutes, it actually took about 2 hours and 30 minutes, as a result of which MHBK could not complete such work by the primary transaction open time, and the transaction open time using the Business Office Terminals on Tuesday, March 15 was extended to 10:25 which was 1 hour and 25 minutes behind the scheduled business office open time of 9:00.

Similarly, due to the repeated suspension of the Night Batch and automated operation on and after Monday, March 14, there were the certain failures because of which lending, loan, foreign exchange and other operations were suspended between Tuesday, March 15 and Tuesday, March 22, and loan modifications and full loan collection operations were suspended between Tuesday, March 15 and Friday, March 25, respectively.

(b) Delays in Opening Transactions on Wednesday, March 16 and Thursday, March 17

On Wednesday, March 16, MHBK suspended the Night Batch for Tuesday, March 15 and started to prepare for launching the Business Office Terminals and implement the DJS Switching necessary to launch the Business Office Terminals. As a result, it became necessary for MHBK to implement the transaction inhibition operations similarly as it did on the previous day. In addition, the ATMs were out of service between 8:00 and 9:33 on Wednesday, March 16, as explained below, MHBK had to respond to these ATM troubles, in addition to its many transaction inhibition operations. For this reason, it took time to launch the Business Office Terminals, and the transaction open time using the Business Office Terminals on Wednesday, March 16 was extended to 11:12 which was 2 hours and 12 minutes behind the business office open time of 9:00.

On Thursday, March 17, MHBK was supposed to suspend the Night Batch at 5:30 based on its experience of the delays of the business office open time it had on the previous day and the day before that so that the delay might not occur, and to

launch the Business Office Terminals on the normal time. However, the ATMs troubles as explained below occurred between 0:00 and 5:20 on Thursday, March 17. As MHBK was required to restore and respond to those troubles, it took time to prepare for launching the Business Office Terminals, and the transaction open time using the Business Office Terminals was extended to 10:46 which was one hour and 46 minutes behind the normal business office open time of 9:00.

C. ATM Outage and Usage Restrictions

As a result of the abnormal end of the Night Batch on Monday, March 14 as explained above, the ATM outage and usage restrictions occurred as described below:

(a) ATM Outage

The suspension and automated operation of the Night Batch for Monday, March 14 as mentioned in Section 4(1)A(a) led to errors such as the failure to implement manual processing necessary for revision of ATM reference dates, and all ATMs were out of service during certain hours between Wednesday, March 16 and Thursday, March 17.

More specifically, in the process of manually processing “revision of the date references used for ATMs” automatically executed prior to 8:00 every day, such “revision of the date references used for ATMs” were not partially executed due to the absence of instructions. As a result, inconsistencies arose between the dates within the ATMs which had been in service on or prior to 8:00 and the dates to which those ATMs referred, making it impossible for MHBK to start its ATM services. Such situation continued until 8:33 when MHBK revised its ATM reference dates and finished work to rerun its ATMs.

Moreover, the “daily online processing” which should have automatically been executed at or prior to 0:00 on Thursday, March 17 was not executed due to the omissions of work, resulting in the inconsistencies of the ATM dates. As a result, the transactions of (approximately 700) customers who made ATM transactions after 0:00 on Thursday, March 17 were not successfully concluded, and the “transaction prohibition” code was automatically created, which made the ATM transactions unavailable. In order to resolve the unavailability of ATMs resulting from “transaction prohibition” code, MHBK needed to manually cancel the “transaction prohibition” settings one by one, and took time for this recovery. For this reason, the ATMs remained unavailable until 5:20 on Thursday, March 17.

STEPS was designed to accumulate the transaction records into files every time

a transaction was made and, when the file capacity exceeded the certain level or the certain period of time elapses, to automatically evacuate those records. Although it became necessary to manually evaluate the transaction records as a result of the above-mentioned automated operations, it was omitted. For this reason, the transaction record files accumulated were not evacuated and exceeded the file capacity of the underlying system. Thus, STEPS abnormally ended at 17:30 on Thursday, March 17. As a result, the ATM transactions became unavailable once again, which continued until 21:36 on Thursday, March 17 when the transaction record files were evacuated and the underlying system was restored.

(b) ATM Usage Restrictions

The ATM usage was partially restricted between Wednesday, March 16 and Wednesday, March 23, as explained below.

Wednesday, March 16 and Thursday, March 17: In order to secure the system resources and prevent unsent exchange transactions from increasing as a result that the exchange transactions were left unprocessed due to the extended operations of the Night Batch for Monday, March 14 mentioned above, MHBK suspended all ATM transfer reservations between 15:00 after the closing of its business offices on Wednesday, March 16 and Thursday, March 17, and 9:00 of the following day on each occasion.

As MHBK could not resolve unprocessed exchange transactions until Thursday, March 17, as described in Section4(1)A(h) above, MHBK suspended usage of its branch ATMs between 19:00 on Friday, March 18 and 8:00 on Tuesday, March 22, and of its outbranch ATMs between 0:00 on Friday, March 18 and 7:00 on Wednesday, March 23, with the aim of normalizing the underlying system by securing the system resources and rerunning the stagnant Night Batch.

MHBK otherwise decided to close its ATMs as a result of the recurrence of the delay in the business office open time on Wednesday, March 17 as explained in section 4(1)B(b) and suspended all ATM usage between 8:00 and 10:52 on Wednesday, March 17. Additionally, in order to evade the possible effects of implementation of the Night Batch on the its online operations, MHBK took steps to suspend parts of its branch ATMs between 8:00 and 12:00, and 15:00 and 24:00 on Tuesday, March 22, putting its emphasis on its responses to recover the delay in the exchange transaction processing.

D. Direct Channel Usage Restrictions

As described in section 4(1)A(h), MHBK took measures to impose EB usage restrictions for Mizuho Direct, Mizuho e-Business Site and Corporate EB in order to secure system resources and implement the uncompleted Night Batch, with the aim of responding to the extended operations of the Night Batch, including the unsent exchange transactions. More specifically, the usage of Mizuho Direct was restricted between 14:30 on Wednesday, March 16 and 10:30 on Thursday, March 17, and between 14:30 on Thursday, March 17 and 12:00, Tuesday, March 22, the usage of e-Business Site and Corporate EB was restricted between 8:00 and 11:30 on Wednesday, March 16 and Thursday, March 17, and between 19:00 on Thursday, March 17 and 12:00 on Tuesday, March 22.

E. Other Events That Affected Customers

(a) Lack of Transaction Details

Because the Night Batch delayed as a result of the occurrence of the Failures and in the course of responding to the situations, STEPS could not provide the Corporate EB and other related systems with some of the transaction details, and the related system lacked some of the transaction details. For Corporate EB, it became partially impossible to make inquiries about remittance/withdrawal details, and customers of this service could not identify remittances and withdrawals between March 15 and 22. This event affected, among others, the contract processing of insurers, finance and settlement of accounts of enterprises, and processing of remittance of university entrance fees.

In response to these, MHBK has continued to take measures to return the lacking transaction details to its customers who requested it as of Saturday, April 30.

(b) Inability to Process Funds Transfer, Return of Data with Erroneous Results, and Processing Omissions

There were the situations where MHBK became unable to create parts of the account funds transfer result data for Tuesday, March 15 and Wednesday, March 16 for nearly 400 companies and data with erroneous result data was returned to its customers.

In addition to the event relating to the return of the above-mentioned data with erroneous result data, there were certain processing omissions resulting from the failure of MHBK to take steps it should primarily have taken, including verifications of the balances payable and the account holders in connection with the certain account funds transfers for Wednesday, March 16 and Thursday, March 17.

MHBK partially reran the processing omissions for Wednesday, March 16, and gave responses to those for Thursday, March 17 separately for each individual company. MHBK returned to the relevant customers the data with precise results for Tuesday, March 15 and Wednesday, March 16 prior to Tuesday, March 29.

(c) Other Defects in the Transactions Associated with the Suspension of the Night Batch

In connection with the occurrence of the Failures, the Night Batch was suspended after the manual DJS Switching at 7:17 on Tuesday, March 15, leading to delays in the processing collection of loan repayments in the lending business, automatic renewal and withdrawals of foreign currency time deposits, automatic withdrawals of time deposits, and collection of fees and commissions as a result of the suspension of the Night Batch.

Although investigations into the effects and modifications of transaction terms resulting from such delays in processing have been almost resolved, MHBK still continues to take responsive actions for parts of collections of fees and commissions as of Saturday, April 30.

(d) Non-collection of Special Payments

As the alternative measures against the ATM usage restrictions in section 4(1)C(b), MHBK took measures to make special payments. However, MHBK made special payments in excess of the deposit balances. As a result, approximately 390 million yen in cash temporary payments made by MHBK at its business office counters was left uncollected as of Thursday, April 28.

(2) Subsequent Measures for the Event That Occurred

In order to minimize the inconvenience of its customers, MHBK made prompt releases of the fact that the failures occurred (A. Public Announcement); gave instructions as to how to respond to customers' inquiries about system failures and services provided (B. Responses at Business Offices and Call Centers); analyzed the side effects on customers resulting from the Failures (C. Analysis of External Effects), and prepared the "List of Items to Which MHBK Needs to Respond for Customers" (as of Saturday, April 30, MHBK still continues to take responsive actions).

A. Public Announcement

Since Tuesday, March 15 when MHBK was delayed in launching the Business Office Terminals, MHBK successively conducted public relation activities through a total of 8 press conferences in which the President & CEO and other executives were present, correspondences to the media, and announcements on its website. MHBK also timely informed the Zengin Center of the delays in connection with the Zengin System, and released correspondences and telegrams of the failures to other member banks in bulk.

As to the timing of public announcement, there were several delays. MHBK announced the delays in launching the Business Office Terminals it could have predicted before opening its business offices at 9:00[5] at which time those business offices opened, on three out of the four times, namely, Tuesday, May 15; Wednesday, May 16; and Wednesday, May 17. In addition, MHBK announced the planned ATM usage restrictions after 16:20 for those imposed at 15:00 on Wednesday, March 16, and after 15:20 for those imposed at 15:00 on Thursday, March 17, out of four times in total. Furthermore, in the public announcements on its webside, MHBK used the expression "restored" on Tuesday, March 15 and Wednesday, March 16, although its services were then just temporarily available. However, it was revised to the expression "(failures) partly resolved."

B. Responses at the Business Office and Call Centers

With respect to the responses at the business offices, the Business Operation Service Promotion Department, the Business Operation Planning Department and other relevant organizations issued instructions and correspondences as to the status of failures and responses associated with the implementation of the business contingency plans periodically after Tuesday, March 15. As for the call center services, MHBK assigned one devoted staff to the Personal Marketing Department so that inquiries from the call centers could be centralized, and prepared and distributed Q&A materials. In addition to the normal call centers, MHBK additionally installed the dedicated call centers for each purpose, such as the call center alternative to inquiries about crediting/debiting details for Corporate EB.

C. Analysis of External Effects

In order to fully comprehend the effects of the subject system failures on its customers, on Wednesday, March 23, MHBK organized a new operation working group (hereinafter referred to as the "Operation WG") under the control of the System Failures Emergency Measures Task Force (hereinafter referred to as the "Failures Countermeasures

[5] Simultaneous releases to the media occurred around 9:00, and the public notification was posted on the website just before or after 9:50.

TF"), and gathered information by assigning staff members of the Operation WG to the business office counters, call centers and other organizations where they could listen to their customers.

As a result, the Operation WG identified the "Events Affecting Customers," and controlled the status of responses to each of those events through subsequent meetings of the Failures Countermeasures TF. After that, Events Affecting Customers was reorganized as the "List of Items Necessary for Customers" after subdividing the events to control the status of responses within MHBK. As of Saturday, April 30, 36 items are under control.

Of the deadlines for responses under the List of Items Necessary for Customers, 21 items have been completed, and 15 items remain uncompleted. Of the uncompleted items, 6 items are to be completed by the end of May; 1 item is to be completed by the end of August; the deadlines for the 4 items which need to be responded separately for each customer have been designated; and the deadlines for the 4 items cannot be designated, because they depend on how the IT & System Division and MHIR respond to them. In terms of content, 8 items relate to the delays in returning data and dispatching documents to customers; 3 items relate to payments of various costs and expenses of fee and other balances requested by other settlement banks; 2 items relate to compensations for interests due to delays in credit or processing; and 2 items relate to repayments of fees due to the unavailability of services.

(3) Management Involvement with the Failures

After the abnormal end of the Night Batch due to the immense volume of transfers to the donation account <a> which occurred at 22:07 on Monday, March 14, the IT & System Division informed the executive in charge of the IT/System Group of the occurrence of failures around 3:30 on Tuesday, March 15.

At or around 5:00 on Tuesday, March 15, the executive in charge of the IT/System Group directed to launch the Business Office Terminals by the business office open time. Although MHBK subsequently attempted to restore the underlying system, it became highly unlikely to commence transaction on time. For this reason, the manager of the Business Operations Promotion Department implemented the business contingency plans for special payments, and lending and foreign exchange businesses at 9:00, and directed the Release Op for after-settlement transfer processing at or around 12:30.

At around 7:00, the executive in charge of the IT/System Group and the IT & System Division informed the President & CEO and Vice President of the conditions of the Failures and their emphasis on launching the Business Office Terminals.

Whenever the situations subsequently changed, the executive in charge of the IT/System Group and the IT & System Division informed the President & CEO that they opened the Business Office Terminals late at 10:25 on Tuesday, March 15; that parts of the exchange transactions were left unsent at around 17:00 due to the delayed implementation of the Night Batch which had occurred on the previous day; and 380,0006 exchange transactions remained unsent at 21:45. Then, at 22:00 on Tuesday, March 15, the management set up the Failures Countermeasures TF within the Emergency Measures Headquarters which had been set up to respond to the Tohoku/Pacific Offshore Earthquake.

The Failures Countermeasures TF created a Customer Committee, Business Office Countermeasures Office, System Restoration Headquarters, and Authorities/Public Relations/Corporate Communications Committee and the management then consolidated the efforts to draw up response policies on and give instructions as to the Failures under this framework.

At around 6:00 on Wednesday, March 16, the executive in charge of the IT/System Group and the IT & System Division informed the management including the President & CEO that MHBK could not continue to launch the Business Office Terminals, and further that they wanted to complete certain critical Night Batches, even though it may delay launching the Business Office Terminals. In response, the management including the President & CEO agreed, and directed them to endeavor to open the Business Office by 11:00 on Wednesday, March 16, in light of the possible impact on customers.

At 21:00 on Wednesday, March 16, the Failures Countermeasures TF was informed by the executive in charge of the IT/System Group and the IT & System Division that they were struggling to process huge number of unsent exchange transactions which had remained unsolved due to the Night Batch delays since Monday, March 14. In response, the President & CEO directed them to open the business offices at an earlier time on Thursday, March 17 and, if it was impossible to restore the Night Batch within the end of the week, during the three consecutive holidays.

MHBK, however, launched the Business Office Terminals late due to a sequence of failures on Thursday, March 17, and there were unsent exchange transactions. Taking discussions at the Failures Countermeasures TF into consideration, the President & CEO directed to impose ATM and other available services usage restrictions between Friday, March 18 and Monday (holiday), March 21.

At 13:30, Friday, March 18, the Failures Countermeasures TF verified after 10:00 on that day that MHBK could connect to Zengin Center and start to send unsent exchange

[6] It turned out later that it was 310,000 transactions.

transactions, and publicized that they would set up the operation room of the Failures Countermeasures TF on the 22nd floor of the head office building in order to consolidate the offices of the involved personnel which had remained decentralized.

From 19:00 on Friday, March 18 to 20:00 on Monday (holiday), March 21, MHBK continually held a total of 7 meetings of the Failures Countermeasures TF to verify the condition of recovery of the Night Batch which remained stagnant. However, it became highly likely that it would not be restored at or prior to 11:00, Tuesday, March 22. Consequently, the President & CEO continued to impose ATM and other service usage restrictions.

On Tuesday, March 22, the stagnant Night Batch started to be resolved. The meeting of the Failures Countermeasures TF was still held daily to verify the condition of restoration, and took actions, including the establishment of the Operation WG in an attempt to respond to unprocessed transactions.

IV. Analysis of Causes for the Failures

1. Overview of the Analysis of Causes

Examining into the causes triggering various failures based on the facts detected as a result of this investigation, the Failures are considered to be largely attributable to basic mistakes made by personnel in charge before and shortly after the system failures (for example, insufficient recognition of Limit Values, lack of understanding of the underlying system as a whole, and the resulting errors in estimation of restoration work time and judgment of the DJS Switching). However, examining into the causes that triggered such basic mistakes and increased the effects of the failures, the following problems are found: flaws in the system functions; insufficient Information Technology Risk management structure which could not have been prevented; insufficient emergency preparedness in restoration work; omissions of human resource development and assignment; and insufficient management and audit. In discussing recurrence prevention measures, it is necessary to clarify causes of such basic mistakes.

In the sections that follow, from this point of view, we analyze the causes that are behind the failures and increased their effects.

2. System Capabilities

The Core Banking System of MHBK started operations in 1988. After that, the system environment drastically changed. Let us take some examples. Although the service hours of ATMs were then limited, they are now available 24 hours a day. As not only the transaction

channels, including Internet and mobile banking, have been diversified and the volume of information has augmented, but also bankers have been requested to process them in a quicker and more intensive manner, as a result of which time to spend for restoration of system has been on the decrease. Therefore, MHBK should have flexibly responded to changes in the system by way of responses to such changes in the situation. These can be summarized, as follows.

(1) System Processing Unit in Case of Concentration of Large Volume of Transactions

The abnormal end of the Night Batch in connection with Company A's donation account <a> occurred in the course of processing to evacuate the transactions details of that account. Although this processing should have been primarily conducted by separating the transaction details within the scope of the applicable Limit Value, all transaction details in that account were processed in bulk. When MHBK attempted to process the large volume of data under such circumstance, MHBK exceeded the Limit Value and the Night Batch abnormally ended.

The abnormal end of the Night Batch in connection with Company B's donation account <b> occurred in the course of processing to allocate data to the successive Night Batch when there was a large volume of transactions details. Although such data should have been primarily allocated within the scope of the applicable Limit Value, all transaction details of that account were processed in bulk. As a result, MHBK similarly exceeded the Limit Value and the Night Batch abnormally ended.

Now that MHBK has substantially large volume of data to handle, it should have maintained the system capabilities that would enable it to conduct segmented processing based on the applicable Limit Value so that it could flexibly respond to the concentration of large volume transactions. However, MHBK did not take such measures in advance.

(2) System Operation Capabilities during the Extended Operations of the Night Batch

STEPS was designed such that daytime online operation and nighttime batch are in operation alternately. The Night Batch is automatically operated by TARGET. However, in case of a delay in processing the Night Batch, MHBK had to suspend the Night Batch and conduct the DJS Switching, unless it elected to extend the time to launch the Business Office Terminals. However, if MHBK conducted the DJS Switching, it had to put the remaining Night Batch into manual operation, which required much time and effort to handle. In that case, exchange data would be created and sent in bulk after the

Night Batch, which would cause delay in sending exchange transactions.

Therefore, had the persons in charge understood such basic schemes of STEPS and TARGET, and recognized the great risk that might arise in the case of a Night Batch processing delay, they could have taken measures to have such capabilities as they could automatically operate unprocessed Night Batch even if MHBK implemented the DJS Switching in advance.

MHBK examined the above-described measures first in the process of restoration work and started to put them into practice on March 19. If, however, MHBK did this from the beginning, the system failures would have been restored in a shorter time.

3. Information Technology Risk Management in an Attempt to Prevent Failures

The system failures at issue arose because the single processing conducted in the course of the Night Batch exceeded the applicable Limit Value. Such Limit Value has never been reviewed since the underlying system had started to operate, and was not among the periodic inspection items. For these reasons, the persons in charge did not fully recognize even the existence of such Limit Value in the Night Batch. Although MHBK assessed the Information Technology Risk in order to prevent this, MHBK also should have needed to review the inspection items as the business environment changed. However, MHBK could not prevent the system failures from occurring, because of the insufficiencies in the periodic Information Technology Risk assessment and review of inspection items in the Information Technology Risk assessment at the time of deployment of a new product/service.

(1) Periodic Risk Assessment of the Systems in Operation

MHBK conducts self inspections of Information Technology Risks in order to screen out risks to its systems in operation (hereinafter referred to as the “Information Technology Risk CSA”) each year. Control items include checking the applicable system capacity Limit Value. The guidelines for such inspection are set forth as the Guidelines for System Capacity Management, under which it conducted inspections.

Although there were instances in which the failures relating to the Limit Value similar to the subject failures, the inspection items on the list of inspections prepared under the above-mentioned guidelines did not include the Limit Value for the transaction details in the Night Batch that related to the Failures.

In addition, a certain public body issued the survey article regarding the instances of system failures involving the financial institutions, and their countermeasures, in which similar cases of failures resulting from huge volume of transfer transactions and delays in operation of the Night Batch were introduced. However, these cases were not fully

utilized, and MHBK did not reexamine the Information Technology Risk inspection items. MHBK eventually processed the transaction details in the Night Batch while it insufficiently recognized the Limit Value, triggering the system failures at issue.

(2) Risk Assessment in Deploying New Product

The abnormal end of the Night Batch in connection with Company B's donation account <b> resulted from concentration of an immense volume of transfers in connection with the mobile phone-based money remittance service. MHBK, however, could not predict such an immense volume of transfers and take necessary preventive measures.

In deploying a new service, MHBK was supposed to have both the User Department and the system department conduct Information Technology Risk assessment using the Check List for Information Technology Risk relating to New Business or New Product Handling. However, as MHBK could handle the service at issue using the existing system and did not need to develop any system, both departments decided to test only the interfaces of Company B's system and MHBK's system (External Connection System). Although MHBK should have conducted tests including the Night Batch based on the expected volume of data, MHBK omitted a test for the volume of data because it did not develop any new system.

The system department would have needed to stipulate the guidelines to conduct tests of the non-functional requirements which would tend to be omitted as the requirements from the User Department (i.e., requirements for processing capacity, security and failure responses) and examine the methodology of risk assessment for new services without development of any new system.

As the User Department expected an immense volume of transfers to be made when it decided to use the above-mentioned remittance service as the donation account, it made inquiries to the persons in charge of the External Connection System about the acceptable volume of data. It should have made inquiries to any person in charge who could judge the possible effects on the related systems, rather than the person in charge of that particular system. However, no person in charge is identified under the current MHBK rules. For that reason, possible effects on the related system were not checked.

If MHBK had recognized the risks of huge volume of data, made risk assessment based on the predicted transaction volume and conducted necessary tests even in the case where there was no development, or if MHBK had maintained and improved the check process that would enable the person in charge of the relevant system to appropriately judge the possible effects on the related system in response to inquiries from the User Department, MHBK could have prevented the Failures from occurring.

4. Emergency Measures for Recovery

Appropriate emergency measures must be established to enable prompt recovery in an event of failure. Emergency measures had been established prior to the Failures in the form of Business Continuity Management Related Rules. However, the Failures could not be recovered in a prompt manner. The reasons for such delayed recovery are identified as follows. First, emergency measures were not effective. Second, possible events assumed in System Contingency Plan were not sufficient. Third, written procedures for recovery were not effective. The reason that those insufficiencies could not be detected beforehand was that checking procedures and drills could not fulfill their role of checking effectiveness.

In accordance with the Recurrence Prevention Measures of 2002, a thorough check of the existing internal regulations related to the Contingency Plan as well as refinement of the internal regulations pursuant to the check results were conducted, including refinement of System Contingency Plan. However, finding out insufficiencies and making improvements using check lists, as well as conducting assessment of effectiveness by checking of internal regulations were not sufficient in light of conducting in-depth checking of the contents.

The reasons for these measures for recovery having become ineffectual are considered to be as follows. First, the Recurrence Prevention Measures for the large-scale failures in 2002 put emphasis on quality improvement measures for newly developed systems and failure prevention measures. Second, STEPS had been stably operated over the long term. Third, the number of occurrences of failures was in a decreasing trend because of the Recurrence Prevention Measures. Because of these facts, it is considered that MHBK became less attentive and less willing to work on recovery measures.

(1) Emergency Measures

With respect to the emergency measures taken against the Failures, insufficiency in review of risk scenarios, lack of appropriate information sharing, and lack of control function are identified.

In responding to the Failures, although both the systems department and the management did respond to each event occurring, they did not conduct thorough review of the scenarios for the greatest risks assumed at each stage partially owing to lack of information, and this resulted in their making inappropriate judgment. For example, in responding to the failures of charity account "a" on March 14th (nighttime), the systems department did not discuss internally one of the biggest risks, the risk of exchange transactions not being conducted, until the problem became apparent in the evening of the 15th. In addition, in responding to the failures of charity account "b" on March 15th

(nighttime), DJS Switching was implemented as the day before even though they were facing the biggest risk event where Night Batch Processing Delays occurred and unrealized exchange transactions accumulated from the day before, which lead to a worsening of the situation.

With respect to information sharing, insufficient information sharing within MHBK and MHIR is pointed out. At the point of 14th, company B gave information to users department of MHBK that a huge volume of payment by transfer was expected. However, such information was not passed from the users department to IT and systems control department, but was passed directly to MHIR. For that reason, IT and systems control department did not realize this fact until the occurrence of failure related to charity account "b" during the night of 16th. In addition, within MHIR where the information was passed, investigation of possible effects was conducted only with respect to the systems that the informed department was in charge, and the information was not passed to the persons in charge of the Core Banking System (STEPS).

Moreover, because of lack of control function at MHIR, MHIR had difficulties in understanding the whole situation. MHBK was also in a similar situation. However, MHBK could not add staff members from MHBK who could control and manage the situation at an early stage, and could not fulfill its responsibility to control the whole situation. One of the causes for the delay in improvement of the difficult situation due to lack of control function was unclear chain of command between management of MHBK and MHIR in the cases of emergency.

(2) Insufficiency in Events to Be Assumed

The Failures began with abnormal termination that occurred during initial stages of Night Batch Processing. However, a System Contingency Plan assuming the occurrence of such an event had not been prepared. For that reason, the written procedures, "Online Response in Night Batch Processing Delays" which was prepared for assumed abnormal termination that may occur during the final stages of Night Batch Processing had to be applied.

Response for failure occurring at each stage of Night Batch Processing was supposed to be prepared. We identified that assumption for possible failure events with respect to Night Batch Processing was insufficient, even though the system was one of the most important systems covering settlement operation.

(3) Insufficiency in Effectiveness of Written Procedures

Two written procedures, namely, "Response to ABEND in the CMF Aut-booking in

Bulk" and "Online Response in Night Batch Processing Delays" were utilized at the system recovery control room in responding to the Failures. The former written procedures were suitable for cases such as the Failures. However, the written procedures did not take into consideration the time expected to be taken. For that reason, implementation of work was determined pursuant to inaccurate estimate of contents of work. As a result, it required a long time until the work was finished and lead to Night Batch Processing Delays.

At branch office matters control room, ten types of Business Contingency Plans could be implemented within the targeted period of time. However, we found insufficiency in consideration for Business Contingency Plans with respect to special payments and cancellation of double payment by transfer.

For special payments, the management of customers to whom such payments were made was done in the unit of each branch office. For that reason, unlawful payments from multiple branch offices to the same person occurred in the initial stage of the implementation of special payments. Although the risk of occurrence of such unlawful payments had been expected, management procedures for paid customers across multiple branch offices had not been prepared beforehand.

With respect to cancellation of double payment by transfer that was associated with response to unrealized exchange transactions, the procedures instructed to contact the customer after cancellation. However, because of confusions in the field, such communications to the customers were not initiated thoroughly and resulted in cases of complaints. Considering the fact that the branch offices were attending customers in irregular situation, such details should have been included in the instructions made to the branch offices from the control room.

5. Problems with Business Management and Organizational Control

(1) Systematic Human Resources Development and Appropriate Allocation

As the cause of the Failures, the lack of human resources who had the practical ability to analyze the effect of an event to the whole Core Banking System, or who could build a prospect for recovery of multiple failures is identified. For example, IT and systems control department could not fully understand the measures proposed by MHIR with respect to Night Batch Processing and exchange transactions. Moreover, reports made by MHIR were limited to fragmental information of events occurred and were not sufficient for determination of appropriate response to failures. However, IT and systems control department could only make a decision to accept them as they were. In addition, MHBK lacked managerial personnel who could have an overview of the whole system and take leadership in response to multiple failures throughout the series of failures.

Moreover, as apparent from the fact that joint drills by MHBK, MHIR and MHOS assuming system failure have not been conducted, MHBK did not fully recognize the need to develop its human resources through such drills.

It is essential for the systems department to hand over know-how and specifications to new personnel by trying to visualize them. At the occurrence of large-scale failures in 2002, a similar insufficiency was pointed out which was described as, "insufficient organization of various documentations". However, visualization of systems stably operated over the long term was not realized and handing over of know-how concerning such specifications was insufficient.

Lack of adequate human resources was caused by the following reasons. First, after the occurrence of large-scale failures in 2002, MHBK worked on improvement of quality. As a result, the number of failure events related to Core Banking System decreased, and multiple failures such as delay in opening caused by Night Batch Processing Delays that lead to the Failures had not occurred. For this reason, opportunities to gain experience in responding to actual failures at MHBK's IT and systems control department as well as at MHIR decreased. Second, under MHBK's policy, review of the whole design of the existing Core Banking System will be performed at the time of construction of the next generation system. Third, system development at MHIR is generally re-outsourced to developers outside of the group. Fourth, promotion of automation of development and operations lead to decrease in number of opportunities for personnel at systems department to learn practical knowledge of system development and system operations. Moreover, along with retirement of experienced employees, personnel with deep knowledge of system requirements and operations requirements of Core Banking System were concentrated on other large-scale projects. At MHIR, seven years from its establishment in 2004 when it had many former employees of MHBK, the percentage of personnel with practical experience of banking operation is rapidly decreasing because other than being in charge of system development for MHBK, MHIR is extending its services to other companies within and outside the group.

Considering the abovementioned factors, MHBK had to put more emphasis on systematic human resources development measures, periodical drills by both sides of MHBK and MHIR, building of skills to respond to multiple failures through simulation experience, and efforts to enable systematic hand over of know-how on the existing system that require maintenance and stable operation over the long term throughout the whole group.

(2) Effectiveness of Audit

Concerning audit department, insufficiency in systems audit of STEPS, insufficiency in the audit system as a group and lack of utilization of outside audit services are identified.

The problems identified above were caused by insufficiency in activities of internal audit department that resulted in series of required improvement activities not being realized. Such required improvement activities include establishment of appropriate audit plans after indentifying audit-related risks, or actively conducting follow-up work on responses by identifying various problem points and making proposals for appropriate improvement measures. We consider that if an in-depth audit had been performed by internal audit department and outside audit services had been effectively utilized, MHBK could prevent the failures discussed in this report or limit the affected areas by such failures.

A. Insufficiency in Systems Audit for STEPS

Audits are conducted by IT and systems audit room after conducting risk assessment and ranking of areas subject to the audit pursuant to "Guidelines for Assessment / Monitoring of Risk". However, "management structure for systems operation" that caused the failures discussed in this report is assessed as level "MH", "the area where audit is highly required and audit should be conducted in principle", which is one degree lower than the highest degree risks, considering the low-and unchanged level of occurrence of failures. In addition, assessment according to departments and systems rates, "deposits and exchange transaction systems" under the scope of IT systems control as having the second-degree, "R2" risks that makes them subject to audits in 30-month intervals. Although "deposits and exchange transaction systems" will have great effects in case of any system failures, the audit system does not treat them as requiring the highest rank of in-depth audit. From the abovementioned fact, we should state that MHBK had low risk awareness for deposits and exchange transaction systems.

We checked the lists of reports on audits performed for the most recent two years reported by the officers. Among them, a report on internal audit related to the system failures discussed in this report merely states that, with respect to failure recovery drills, "formatting of reports are not standardized" and that, "failure recovery drills are conducted only within operations department". With respect to Contingency Plan, such report merely states that, "management keeping connection with failure response drills is realized, and no problem in consistency was found", and that, "completeness and consistency for the plan as a whole are ensured". These audits may be criticized as focusing too much on formalities. We assume that the internal audits did not assess the points that written

procedures for DJS Switching had not been reviewed for a long time and that there was problem in effectiveness of recovery processing in case of any failures in Night Batch Processing.

B. Audit System as a Group

Regarding MHIR, MHBK only has audit capacity for outside contractor pursuant to outsourcing agreement. In comparison, MHFG has the authority to conduct direct audit of its subsidiary, MHIR. However, in reality, MHFG only receives repots on results of audit by themes and by departments conducted by internal audit department of MHIR, and MHFG's audit department does not conduct a direct audit of MHIR. Moreover, audit by themes conducted by internal audit department of MHIR is targeted at its own systems and payroll calculation services outsourced to MHIR, but is not targeted at STEPS outsourced from MHBK. In addition, systems audit is not conducted with respect to "1st Division, Core Banking, Banking System Group" responsible for STEPS.

As described above, systems audit for STEPS that caused the Failures and for department responsible for STEPS is conducted by MHBK's audit department only, only within the scope of audit services outsourced by MHBK, and no internal audit as a group is conducted to this day.

C. Lack of Utilization of Outside Audit Services

The Financial Institutions Inspection Manual[7] states that, outside audit services shall be utilized as necessary with respect to audit of systems risk management structure, not only with respect to audits of projects such as system integration and large-scale system development. Also, it states that utilization of outside audit services as one of the Recurrence Prevention Measures developed pursuant to the large-scale failures in 2002.

However, cases of utilization of outside audit (assessment) services by audit department after the occurrence of the large-scale failures in 2002 were limited to utilization at the planning phase of branch offices transfer project in 2003 where such audit was conducted jointly with the audit department under Co-Sourcing Method, and utilization as advisory services for internal audit department at the transfer phase of the project in 2004. There was no case of utilization where the whole systems risk management structure was assessed, apart from project audits. It can be stated that complementation of insufficient audit by internal audit department by utilizing outside audit services is not realized. Systems risk control room of IT and systems control department utilized outside audit services three times from 2005 through 2007. However,

[7] Formally called, "Manual for Inspection of Depositary Financial Institutions "

such information was not shared with the audit department, and the result given by outside audit services was not effectively being utilized.

(3) Others

As described above, there are insufficiencies in areas such as improvement of system function, recovery management structure, human resources development and audit at MHBK. Such insufficiencies are thought to be caused by MHBK not being able to respond to changes in business environment and diversification of systems utilization. MHBK should have always taken control of effects of business changes to the current systems as an organization, and should have timely conducted measures for improvement of systems and audit system, and should have taken measures for human resources development and securing.

Looking back at the Recurrence Prevention Measures for the large-scale failures of April 2002, although the cause of this previous event of failure is not directly related to the cause of the Failures, if MHBK learned from such previous large-scale failures and paid attention to stable operation of computer systems as an organization, MHBK could have prevented the Failures.

V. Proposal for Recurrence Prevention Measures

1. MHBK's Recurrence Prevention Measures

On April 28, in response to the Failures, MHBK established the "Root Cause Analysis, Improvement and Countermeasures on System Failures" (hereinafter referred to as "Recurrence Prevention Measures").

In the Recurrence Prevention Measures, MHBK indicates that the Failures occurred in the context that (i) MHBK was not sufficiently aware that "a concentration of transactions on a particular account can cause an abnormal termination of the processing of the Centralized Ledger in Center" and "this involves a risk that various operations are consequently affected," and states that (ii) the occurrence and aggravation of the Failures was caused by the following two factors: "MHBK failed to develop adequate approaches to prevent an abnormal termination of the processing of the Centralized Ledger in Center that can occur when transactions concentrate on a particular account" and "MHBK did not demonstrate appropriate responses and actions after the abnormal termination of the processing of the Centralized Ledger in Center" due to the above-mentioned insufficient awareness.

In light of the above, MHBK looked into the cause of the Failures in further specificity and detail, and formulated the following Recurrence Prevention Measures:

(1) Measures to Prevent Information System Failures Similar to Those at Issue

A. Improvement Measures Concerning "Approaches to Prevent Occurrence of Failures"

(a) Review, management and strict control of the procedures for the accounts through which a large volume of transactions are expected to be conducted;

(b) Revision of the Limit Value for the Centralized Ledger in Center within the deposit system and monitoring of large volumes of data;

(c) Establishment of operations and risk control that are conscious of the Limit Value on a product-by-product basis;

(d) Measures to improve the design and specifications of the Centralized Ledger in Center within the deposit system; and

(e) Enhancement of assessment of the Information Technology Risk at the time of development of new products and services.

B. Improvement Measures Against "Inappropriate Responses and Actions to the Failures"

(a) Specifications of the time limit for the Centralized Ledger in Center and identification of possible impact of the failures thereof;

(b) Better response to large volumes of data that could lead to an abnormal termination;

(c) Streamlining of measures to deal with delays in the processing of the Centralized Ledger in Center;

(d) Determination of the scope and coverage of the critical settlement operations and other operations of high quality, identification of the actions to be taken, possible impact, restrictions, order of task priority, among other matters, and establishment of procedures for each operation;

(e) Implementation of systematic training that contributes to enhancement of human resources;

(f) Establishment of a system to call on people who have considerable know-how and experience in case of emergency;

(g) Revision of systems so that they can effectively function in case of emergency;

(h) Appropriate instructions to the branch offices and postings on the Internet website and other media based on accurate information;

(i) Tracking and analysis of complaints, grievances, etc. and study of

countermeasures and improvement plans; and

(j) Fair treatment of claims for reimbursement of actual costs or compensation for damages incurred as a result of information system failures.

(1) Measures to Improve Information Technology Risk Management System

A. Enhancement of System Risk CSA

(2) Measures to Improve Business Continuity Management System

A. Improvement of Systems to Respond to Emergencies

(a) Revision of the internal emergency response system;

(b) Revision of communications and information sharing flows immediately after the occurrence of an emergency;

(c) Implementation of emergency response training for directors, officers and employees; and

(d) Verification of the effectiveness through bank-wide training as preparation for information systems failures.

B. Enhancement of System Contingency Plan

(a) Clarification of the contents of the System Contingency Plan;

(b) Implementation of mock training to increase the effectiveness of the System Contingency Plan.

C. Enhancement of Business Contingency Plan

(a) Re-examination and review of the Business Contingency Plan;

(b) Strict compliance with the guidelines that apply upon the exercise of the Business Contingency Plan;

(c) Communication with the branch offices regarding the required actions upon the exercise of the Business Contingency Plan and implementation of training.

MHBK states that in light of the results of the inspection by the Financial Services Agency and the Committee's opinions and recommendations, it will continue verification of the adequacy of the above-cited improvement measures and consider further improvement measures, as appropriate. MHBK acknowledged its commitment to make continued efforts to enhance the Information Technology Risk management system and the business continuity management system.

2. Assessment of Recurrence Prevention Measures

The Committee assesses MHBK's Recurrence Prevention Measures as basically adequate. This is because they openly admit that their insufficient awareness of the Information Technology Risk was one of the causes of the Failures, and considers not only measures to prevent recurrence of information system failures that are similar to the Failures but also a framework to manage Information Technology Risk in general. That said, the investigation by the Committee identified the following issues that would require further consideration:

(1) Management System for Prevention

A. Lack of Measure to Ensure Effectiveness of Evaluation of Enhancement of System Risk CSA

The Recurrence Prevention Measures indicate, for enhancement of the System Risk CSA, the need to set a maximum allowable transaction volume and review the system specifications and the controlled items with special focus on the BtoC area through cooperation among the Systems, Products and Administration Divisions. Meanwhile, it is also necessary to consider how to improve the effectiveness of the evaluations.

B. Need to Strengthen the Information Technology Risk Management Procedures upon Introduction of New Services

While the Recurrence Prevention Measures mention the need of enhancement of evaluation of the Information Technology Risk at the time of introduction of new services, the Committee believes that MHBK also needs to conduct tests that assume processing of a large volume of data to handle a large number of deposit transactions made on a particular account, even if such services do not involve any systems development.

(2) Management System for Early Recovery

As to the emergency response systems, the Recurrence Prevention Measures mention, as an improvement measure, a revision of the personnel's roles and information sharing within MHBK as well as the revision of the roles and information sharing among MHBK, MHIR and MHOS.

As for the addition of possible events for which MHBK should be prepared and the securement of the effectiveness of the procedure documents, the Recurrence Prevention Measures point out the necessity to develop a Contingency Plan and procedure documents assuming information system failures similar to the Failures and to proceed to work on a fundamental improvement after reviewing the risk scenario and clarifying the matters to be set forth in such a Contingency Plan and procedure documents.

Furthermore, the effectiveness of such Recurrence Prevention Measures is supposed to be verified through training within MHBK as well as cross-company training among MHBK, MHIR and MHOS.

While specific methods and process of the revision of each of the above-mentioned issues are yet to be considered, the Committee evaluates the above-described measures to be appropriate as a basic direction.

(3) Management of Business and Organization

A. Personnel Measures

As to the measures to enhance human resources, MHBK intends to ensure consolidation of knowledge and know-how as well as reinforcement of the management through systematic training programs to enhance the workforce. While specific plans are yet to be considered, the Committee assesses such measures to be appropriate as a basic direction.

B. Internal Audit

With respect to the internal audit department, MHBK intends to have it gain better understanding of potential risks and more diverse perspectives, and this is appropriate as a basic direction. However, improvement of the audit method in the internal audit department is critical in view of the fact, among others, that the internal audit failed to identify the problems in the effectiveness of the procedure documents. This point is as specifically indicated in the Committee's recommendations below.

3. Proposals on Recurrence Prevention Measures

(1) System Function

In the course of re-checking of Information System Contingency Plan and Business Contingency Plan, it is necessary to consider whether risks identified fully cover the potential risks. For such purpose, MHBK must re-check and re-analyze the current systems for existence of possible risks related to system design and system operational design other than those identified in relation to the system failures discussed in this report, and if any, MHBK must include them in risk scenarios of contingency plans.

(2) Management Structure for Prevention

A. Improvement of Effectiveness of Information Technology Risk CSA

MHBK performs an annual risk assessment pursuant to check lists for each system, which is called Information Technology Risk CSA. We consider that improvements in

preciseness of checking procedures are also required as well as improvements in items in the check list, in order to enhance effectiveness of the risk assessment.

In order to improve items in the check lists, it is necessary to perform continuous and multidimensional risk assessment taking into consideration both internal and external environmental changes instead of merely referring to common standards referred to by financial institutions. To achieve such purpose, we advise that MHBK actively utilize viewpoint of those outside the bank, in addition to internal viewpoints of the bank such as product management, operations and systems departments.

Moreover, in order to improve preciseness of checking procedures, MHBK should not be satisfied by checks performed under the responsibilities of departments in charge of systems alone, but also needs to perform cross-checking of appropriateness of check results among multiple departments and conduct reviews with vendors and outside experts in order to realize comprehensive checking from multiple viewpoints. Moreover, Information Technology Risk Department must go beyond routine confirmation of check results and consider on-site verification.

(3) Management Structure for Early Recovery

A. Proposal on Review of Emergency Measures

The important points in review of emergency measures are realignment of the roles of each organization, clarification of the existence and scope of responsibilities of each organization, and establishment of chain of command at field-level, and, in addition to that, establishment of an integral chain of command that includes respective top management of MHBK, MHIR and MHOS.

B. Proposal on Fundamental Improvement of Information System Contingency Plan and Procedures

To realize fundamental improvement, it is important to sort out potential flaws in effectiveness in the current Information System Contingency Plan and Procedures (risk scenarios that are lacking, potential omission in written procedures, scope of required automation and other issues). We consider that review by cooperating with outsourced entities such as MHIR and utilization of outside experts are effective for resolving such flaws.

Moreover, to continue such improvement efforts rather than making it a one-time event, MHBK must review the current method of conducting periodical checks of and making improvements to Information System Contingency Plan and Procedures so that such checks will go further to consider appropriateness of the contents of such plans and

procedures. We advise that during such review the three companies consider together ways to realize horizontal checks of written procedures that are within the scope of MHIR and MHOS, in addition to those within the scope of MHBK.

(4) Business Management and Organizational Control

A. Human Resources Development

MHBK and MHIR shall work on systematic human resources development, conduct periodical drills on both sides, develop skills required for handling multiple failures through simulation experience, and reinforce their effort to systematically hand over know-how on the current systems which requires a long-term maintenance and stable operation within the whole group.

(a) Short-Term Measures

MHBK must promptly prepare risk scenarios in a focused way and must conduct failure response drills in order to enhance human resources development and skills. In particular, test of effectiveness of various improvement measures by drills conducted assuming the reoccurrence of the Failures is essential.

Prior to such drills, joint planning by MHBK and MHIR must be done. Such plans shall specifically include improvements on risk scenarios that must be made to supplement scenarios lacking due to the systems stability in operations over the long term. Such plans shall also include the establishment of desirable structures and roles of management and field levels in responding to failures, and points to be reviewed at drills. Moreover, drills for respective risk scenarios must be held in order to test effectiveness of the contents of the planning. Particularly, drills and testing of effectiveness must be repeated periodically for their sophistication.

After such drills have been conducted and tests on effectiveness have been made, a series of process including review of risk scenarios, determination of drills to be held periodically and on an ad hoc basis as well as establishment and documentation of failure response procedures is required.

(b) Medium to Long-Term Measures

In addition to the short-term efforts listed above, management must acknowledge the medium to long-term viewpoints and reacknowledge the importance of systems department and activate personnel exchanges between MHBK and MHIR. Moreover, by conducting systematic human resources management of not just MHBK but also the whole group, MHBK must develop human resources who are able to

conduct management with understanding of the full picture of banking business and systems.

B. Audit

(a) Risk Assessment for MHBK Core Banking System (STEPS)

"Deposits and currencies systems", that are under the scope of IT systems control for the purpose of evaluation of departments and systems, are evaluated as having the second-degree of risk and are subject to audits in 30-month intervals. However, considering the importance of such systems, we advise that such audits be conducted as those for the highest degree risks in a more thorough manner, such as by checking the effectiveness of manuals and referring to similar cases of failures in the past.

After giving appropriate evaluation of effects when the risk events occur, MHBK must review the method of risk assessment by audit department prepared at the time of planning.

(b) Audit System as a Group

We found insufficiency in the audit system as a group for audit of MHIR concerning Core Banking System (STEPS). Therefore, review for enhancement of the audit system of the whole group including the clarification of the role and position of the audit department of MHFG, such as by considering direct audit by audit department of MHFG or increasing the scope of internal audit by MHIR is required.

(c) Utilization of Outside Audit Services

It is understood that MHBK will put its efforts into comprehending potential risks related to Core Banking System (STEPS) and into enhancing points of audit concerning systems such as STEPS. In order to realize this, increasing the skill of personnel in charge of audit and utilization of outside audit services need to be considered.

4. Proposals for Future

Customers' trust for MHBK's systems has been damaged by system failures discussed in this report. Computer systems of major banks are economic infrastructures. Therefore, any damage to such infrastructures has a large effect to their stakeholders including their customers. Not only MHBK but also the whole Mizuho Group must put their greatest efforts into maintenance of such infrastructures and recovery of trust. Fortunately through this investigation,

we could see determination of persons concerned at MHBK to restore trust. However, once-damaged trust cannot be easily recovered. From such a viewpoint, the Committee addresses the next two points as our conclusion and proposals for the future.

The first point is continuous implementation of preventive measures.

In response to the large-scale failures in 2002, Mizuho Group established the preventive measures and it was evaluated that these measures had accomplished their initial objectives by 2004. However, Mizuho Group once again caused system failures this time. Although the system failures this time occurred in different situation from that of 2002, if Mizuho Group as an organization paid attention to stable operation of the systems learning from the failures in 2002, Mizuho Group could prevent the system failures this time. Preventive measures will not become meaningful until they are actually implemented and such measures must continuously be implemented over the long term. A long-term, continuous implementation of the preventive measures with maintained determination for recovery of trust is highly desirable.

The second point is prompt realization of system integration.

Currently, MHBK and MHCB are in a same group. However, they operate separate systems as from the time prior to consolidation. However, existence of demerits of such separate systems is clear. Therefore, also from the viewpoint of cost reduction in the long-term as well as improvement of systems, integration of systems in the whole group is desirable. "Mizuho's Transformation Program" issued in May 2010 clearly states promotion of unification of IT and systems in the group. Taking the system trouble discussed in this report as an opportunity, MHBK must carry out thorough preparation for prompt realization of unification as stated in the above program, which would lead to earlier recovery of trust of the customers.

- End -

Appendix A

List of Terms (System Terms / MHBK Terms)

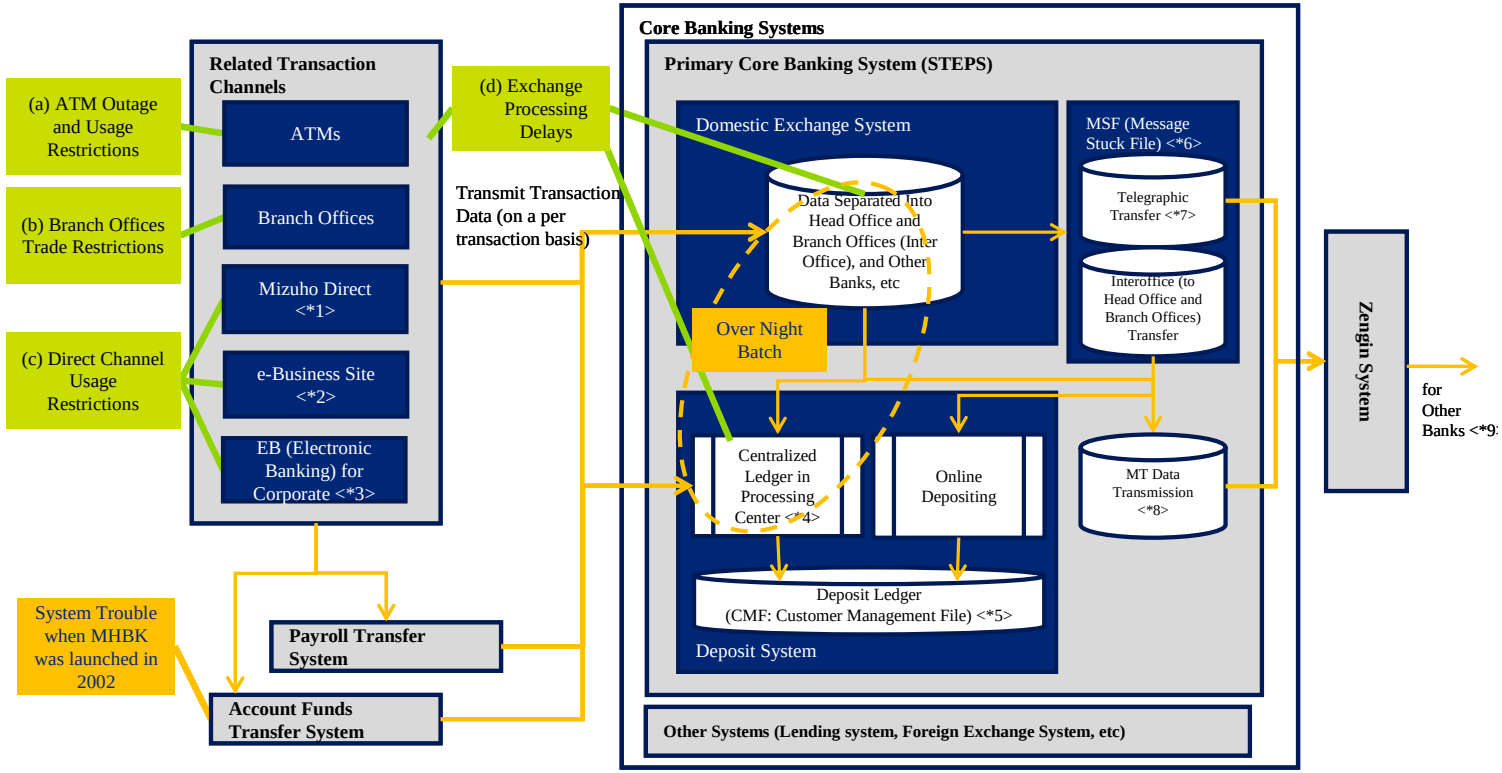
Terms	Official Name / Description
ABEND	"ABEND" is short for "Abnormal End". There are two kinds of "ABEND": (1) System "ABEND" occurs to secure the system when the system lacks resources to process a job or a job times out, etc. (2) User "ABEND" occurs when a logical contradiction exists in the code and the program terminates.
ATM	"ATM" is short for "Automated Teller Machine", which is used to process cash deposit and withdrawal.
BtoC	"BtoC" is short for "Business to Consumer", which is a kind of Electronic commerce (EC) that describes activities of businesses serving end consumers with products and/or services.
CMF	"CMF" is short for "Customer Master File", which is a file that saves the balance of deposit transactions for customers, etc.
CSA	"CSA" is short for "Control Self-Assessment", which is a process designed to make executive level managers and field level staff continuously aware of the risks and related controls affect the possibility of achieving the objectives of the organization, and to make appropriate adjustments as a result.
EB	"EB" is short for "Electronic Banking", which is a generic service provided by MHBK for customers to make transfers and tax payments, etc with terminal operations out of bank offices.
EBIS	"EBIS" is short for "Electronic Banking Integrated System", which is a system that executes various banking transactions such as transfer and inquiry, and provides Mizuho FB (Farm Banking) service that includes calculation features for contract management, Settlement funds acceptance/return, and commission.
e-Business Site	Mizuho "e-Business Site" is a service to connect corporate customers' PC to Web systems of Mizuho Bank and Mizuho Corporate Bank via the Internet, and execute various banking transactions such as transfer and inquiry.
Branch Office Terminals	Operation terminals used to execute interface and deposit/withdrawal, issuance of passbook, etc for settlements in branch offices.
Off-Site Backup System	Backup method wherein the backup system is installed and operated in a different location from the primary system environment. The off-site backup system is developed for system failure caused by large-scale disasters such as earthquakes, etc..
Online Processing	Processing method wherein transactions are processed one by one in real time, immediately updating system databases. (As opposed to Batch Processing which pools transactions and processes a batch of data at one time.)
Transfer instruction with withdraw booking from customer account	Transfer instructions that the fund has not yet withdrawn from customer account.
Core Banking System (STEPS)	"STEPS" is the name for the MHBK Core Banking System, which is the system that processes business deals with customer's settlements such as deposit transactions (e.g. deposits, payment, etc) and loan transactions (e.g. loan, repayments, etc), foreign exchange transactions.
Account Funds Transfer System	A generic system that executes settlement funds acceptance/return and due date management, etc.
Co-Sourcing Method	Internal audit staffing model wherein an outside consultant is hired to jointly execute internal audit work to compensate for lack of personnel and/or expertise in the internal audit department.

Terms	Official Name / Description
Contingency Plan	Pre-defined measures or action steps in order to minimize damage and loss due to adverse contingencies such as incidents, accidents, disasters, etc.
Information Technology Risk	The risk that a financial institution will incur loss because of a breakdown or malfunctioning of computer systems or other computer system inadequacies, or because of improper use of computer systems.
Automatic Operation System (TARGET)	"TARGET" is short for "Total Automatic operation for Reliance GEnerate Tool", which is a system to start batch jobs and support disaster recovery in the case of file failure. It is based on a general automatic operation management system provided by Fujitsu. It is used for automatic operation to control over night batch processing in STEPS.
"SHIMUKE" (Outbound Instruction)	"SHIMUKE" refers to sending customer's requests such as remittance, transfer, etc to other banks. (As opposed to Inbound instruction)
Securities/Market System	A generic system name composed of system features required to trade securities and derivatives.
Information Support System	A generic system name to provide information required for business operation, and information related to risk management, based on data from Core Banking System.
Zengin System	System that executes domestic exchange transactions in online processing with computers and communication lines in Japan.
Centralized Ledger in Center	"Centralized Ledger in Center" is a mechanism to process large volumes of various data (e.g. account funds transfer, salary payment, periodic replacement certificate, etc) in bulk based on contracts with customers.
Payroll Transfer System	A generic system name to make general transfers and payroll transfers.
External connection System (Customer)	A generic system name composed of system features required to connect to external systems and provide services to customers. For example, ATM, e-Business Site, EB (Electronic Banking) for Corporate, etc.
Direct Channel	Transaction channel for customers to make banking transactions directly via the Internet, etc.
"DAKEN" (Input)	Manual data entry using the Branch Office Terminals.
Over Night Batch	A processing method wherin transactions are pooled together and processed in batches to update system databases. (As opposed to Online Processing, which processes transactions one by one in real-time.)
Daily Processing (DJS Switching)	"DJS" is short for "Daily Job Schedule," which is an automated process that updates scheduled batch jobs to execute on the following day after successful completion on the current day.indicating the "centralized ledger in center" process has been updated.
"HISHIMUKE" (Inbound instruction)	"HISHIMUKE" refers to accept other bank's request such as remittance, transfer, etc. (As opposed to Outbound instruction)
Mizuho Direct	Services for individual customers to make transfers and settlements, etc 24 hours a day via the Internet. For example, Internet Banking, Mobile Banking, Telephone Banking.
Limit Value	The Limit Value represents the system processing capacity limitation where system processing becomes inefficient and can lead to system problems or failure.

Terms	Official Name / Description
Relay Computer	A generic system name used to connect to different systems.
REEF account	This account uses a reef instead of passbook and certificate etc. Specifically, the Center Reef Account created in the operation center can minimize the amount of transaction record that is archived at information systems since it doesn't keep detailed transaction logs.

Appendix B

Conceptual Chart of MHBK's System



<*1> Service for individual customers to make transfers and settlements, etc 24 hours a day via the Internet.
<*2> Service for corporate customers to make remittances of domestic/foreign exchange transactions and inquiries of transaction information, etc via the Internet.
<*3> Service for corporate customers to make transfers and inquiries of transaction details, etc with general purpose computers, PCs, dedicated terminals.
<*4> TARGET system processes a centralized over night batch job containing MT data and transmission data, etc from customers (does not include online processing at ATM and branch offices)
<*5> File to save the balance of deposit transaction for customers, etc.
<*6> System to save exchange data, and connect with the Zengin.
<*7> One trade method to execute exchange transactions via the Zengin. Telegraphic Transfer processes the majority of the total transaction volume of transfers for other banks
<*8> Processing method to send large amounts of data in bulk to the Zengin.
<*9> The above data flow is applicable to exchange transactions as sending banks only.