Supervisory Bureau No. 1515
June 3, 2008

To: Financial Institutions Handling Deposits, etc. and Related Organizations

From: Masao Nishihara, Director-General,
Supervisory Bureau of Financial Services Agency

Regarding System Risk Control at Financial Institutions

Financial institutions' computer systems constitute the core element of payment and settlement systems as a whole, which entails their highly public nature as an integral part of the social infrastructure of any given economy. Should any glitch, failure, etc., occur therein, it could cause significant damage to their users' socio-economic livelihood, the economic activities by corporate and other entities and eventually to our country's economy as a whole.

As one of its priorities under the "Guidelines to the Oversight and Monitoring, etc., for Business Year 2007" published in August 2007, the FSA established the requirement for assurance of the adequacy of the overall framework for financial institutions'
system risk management, while promoting the establishment of a proper structure and procedures for such risk management at all institutions. Meanwhile, in light of the fact that past occurrences of system glitches have, with the ongoing sophistication and increasing complexity of financial institutions' systems, come to represent an increasingly serious threat to the customers of relevant institutions, the bureau also considers it important to build a solid structure to respond to any system glitch or failure in the process of its occurrence in a most prompt and suitable way, in order to limit the damage incurred thereby to the greatest degree possible. Actions toward such causes must be examined, as stipulated under the guidelines.

Under such circumstances, actual system glitches have occurred at several financial institutions in the recent past, causing significant inconvenience to their clients. It has also been a regrettable situation for the bureau and FSA.

The bureau has therefore decided to call for financial institutions operating in Japan to take such actions as those outlined in the attached document, wherein they are encouraged to implement, as part of their forward-looking efforts under the management's proactive leadership, system risk management with full and accurate recognition of the risk circumstances inherent in all such aspects, including future system integration, system/program upgrading, daily maintenance and implementation. Please be advised to ensure that each of your group companies is also fully notified of the following contents.

(Attachment)

Regarding the Control of System Risks at Financial Institutions

As an aspect of recent developments, actual system glitches have occurred at several financial institutions, causing a significant inconvenience to their clients, which the bureau also takes very seriously.

The financial institutions' computer systems nowadays constitute the core element of the payment and settlement systems as a whole, which entails their highly public nature as an integral part of the social infrastructure of any given economy. The restructuring efforts and expansion of tie-up relationships have progressed within the industry over the past few years, and among other things have resulted in an extremely complicated configuration and application of the financial institutions' computer/online systems in general. In addition, higher dependence on the IT facilities of financial institutions' day-to-day operations as well as the extension of the real-time online networks in recent years have led to a situation wherein even a small system glitch can potentially cause relatively greater damage than would otherwise be expected. In consideration of such circumstances, ensuring system stability has become an especially important business objective on the part of financial institutions in general. Today's financial institutions are required to take full precautions against all contingency situations, which are exemplified by the strong initiative taken by the management bodies of institutions in their reinforcement of system risk controls.

The examination of actual cases of system glitches or failures that have occurred recently shows that they have principally occurred 1) in conjunction with the system integration measures taken internally or between/among financial institutions; 2) together with system and/or program upgrade operations, changes to business structures and so on; 3) in the process of daily implementation and/or maintenance procedures. It is therefore important that all financial institutions preemptively evaluate, with reference to these various preceding cases, the potential consequences of any system glitch to their customers while investing their resources so as to ascertain the most effective approaches in regards to this area. Meanwhile, should system glitches actually occur, institutions will be expected to do their very best to ensure the earliest possible recovery of the system and to make conscientious responses to their customers, while displaying proper and highly transparent accountability to society at large in regards to the incident.

Financial institutions are therefore requested to implement full and complete inspections of their computer/online systems in regards to the criteria stipulated below so that the system risk control can be conducted, as part of forward-looking efforts under proactive management initiative, with potential risks inherent in situations such as future system integration, system or program upgrading, daily maintenance and implementation being identified accurately in advance.

Key Inspection Points

(1) Financial institutions' computer/online systems provide the clearing services that involve core elements and activities of the national economy. It should therefore be examined whether or not the management bodies of institutions are administering system risk control with strong initiative, in light of the fact that their clients would be significantly affected by any occurrence of system glitches. In view of the fact, among others, that system glitches have thus far occurred not only in conjunction with system integration measures but also with system upgrades and program renewal as well as the processes of daily application and maintenance procedures, it should also be examined whether or not each institution is undertaking solid measures to alleviate system risks, which should be identified as per each of the above-mentioned situations.

(2) All system facilities and operational or business procedures that could involve risk events whose actual occurrence, despite their low probability, would incur enormous impacts or inconvenience to clients and to the entire clearing system, etc., must be identified in a thoroughly comprehensive manner. It should be examined whether or not the measures to prevent such risk events from occurring have been established in a thoroughly secure manner by the relevant institution, by way of thoroughgoing test rehearsal and so on.

(3) As for other system facilities and/or operational procedures that do not involve the risk events specified in (2) above, it should also be examined whether or not the institution is adopting at least the same types of measures as mentioned above, so that the probability of the occurrence of such risk events would be maintained at under a certain acceptable level.

(4) In preparation for situations where a system glitch or failure has actually occurred, all institutions must be well equipped with an recovery plan and structure, so that the earliest possible recovery can be ensured. In the case of the emergence of any glitch situation, the relevant institution must publicly announce circumstances and causes thereof, the prospect for recovery, etc., while establishing a call center for the purpose of responding to customers in a conscientious manner. Is the institution in question well positioned to make these responses in a prompt manner? Furthermore, in preparation for any situation where manual operations are required until the system's full recovery, the institution must have a framework in place whereby it can secure adequate numbers of staff members upon having identified the extent of the manual work required in an appropriate manner.

(5) Regarding the system risk contingency plan, it should be examined whether or not it includes structures that would enable the institution in question to deal with the diverse circumstances

assumed under various risk scenarios and whether or not the practicability of such a plan has been proved by way of a sufficient number of repeated drills, so as to ensure that the plan does not remain a mere “impracticable theory”.

Past Examples of System Glitch Incidences

* Incidents that occurred in conjunction with system integration

- A case wherein ATM and transfer/remittance services became unavailable due to a system failure that occurred on the interface of exterior and internal lines, or the undercapacity of the operational infrastructure, which did not adequately support the processing of large volumes of transactions, etc.

- A case where system upgrade resulted in a modified transmission format for electronic instructions that was unacceptable by other banks’ systems, leading to temporary ATM failure on the side of partner institutions

Incidents that occurred concurrently with system and/or program upgrade operations, changes to operational structures and so on

- A case where there was a software deficiency in relation to the transmission of data to the “Zengin (Japanese Bankers’ Association) Center”, which caused a failure in clearing a large volume of transactions during regular business hours

- A deficiency that occurred during the system upgrade process wherein the start-up of a back-up computer was triggers but such a back-up functions did not work in the proper manner, resulting in an overall system failure

- A case of duplication of transfer transactions in the process of transferring customer data, wherein the procedures for subsequent data processing were also established but a mistake occurred in the order thereof.

- A case wherein processing volume was temporarily concentrated within a single action or occurrence together with a change in operational structure, wherein the number of system inputs increased sharply to the extent that it exceeded the system’s capacity, resulting in an overall operational processing failure

- A case wherein the online system incurred glitches as a result of mistakes in the process of implementing functional enhancements, resulting in the failure of OTC and ATM processing of deposit and transfer/remittance transactions

* Incidents that occurred in the process of daily implementation and/or maintenance procedures

- A case wherein the server connecting the core system and the outside systems incurred hardware-related problems, resulting in the suspension of ATM transactions with other banks

- A case wherein end-of-the-month transfers far exceeded the system’s capacity, resulting in a situation wherein the settlement of a large amounts of outgoing transfers to other banks were postponed until the next business day