Roger W Ferguson, Jr: Implications of 9/11 for the financial services sector

Speech by Mr Roger W Ferguson, Jr, Vice Chairman of the Board of Governors of the US Federal Reserve System, at the Conference on Bank Structure and Competition, Chicago, Illinois, 9 May 2002.

* * *

Good morning. It's been seven months since the attacks on the World Trade Center. Today, I would like to discuss my thoughts on business resumption planning after 9/11 and some implications for the financial services sector.

Financial services firms in and near the World Trade Center were severely affected by the 9/11 attacks. The industry experienced an unprecedented loss of lives and property, requiring massive, long-term relocations to contingency sites and dedicated efforts to protect and reassure staff. The destruction of telecommunications infrastructure supporting lower Manhattan disrupted the telephone connections for several days between the whole nation and financial markets and intermediaries located in the lower Manhattan financial district. This disruption created bottlenecks in the processing of financial transactions and caused a temporary--but severe--dislocation of liquidity for financial institutions. The primary markets closed temporarily, to facilitate disaster-recovery efforts and to ensure fair and orderly markets, until telecommunications could be restored.

Despite the shock, long-term devastation, and disruption of public infrastructure and commercial activities in the world's financial center, the U.S. financial system largely remained open throughout the day and thereafter. Banks and other financial intermediaries stayed open. Key wholesale and retail payments system remained operational, like other financial activities, except to the extent that telecommunications disruptions had a temporary or local effect. Even firms in the World Trade Center were able to resume business from other offices or from contingency sites within hours of the attack. The response of the financial industry and the speed with which it resumed business was extraordinary and can be attributed only to its long-standing commitment to, and extensive preparations for, ensuring continuity of operations in the wake of physical and cyber disruptions.

Why did the financial system perform so well, and what can be done to ensure the smooth operation of the financial system if wide-scale disruptions recur? These questions are receiving continued scrutiny within government agencies and among industry members, and are the subject of extremely useful discussions, which I think will result in a more secure and resilient financial system.

Preparedness of the financial services sector

Financial institutions and markets were able to recover quickly from the 9/11 tragedy for several reasons. First, the financial industry incorporated information technology into its business processes many years ago and since then has encouraged innovations in business process to achieve efficiency and security. As a result, industry participants are extremely knowledgeable about technology and the related operations risk.

Second, financial institutions understand that it is in their best business interest to make business continuity planning an executive management issue, requiring top-level involvement and not insignificant investment. Preparations for the century date change gave us a much clearer understanding of the financial system's dependence on technology and on the complexities of managing operations risk. Once institutions understood the considerable business risks that would result if they could not serve customers, they moved the management of Y2K preparations out of the back office and onto the desks of product-line and senior managers. Firms understand that they must manage not only business risks flowing from operational issues but also inherent reputational and legal risks.

The century date change provided other benefits as well. In preparing for Y2K, financial institutions modernized and incorporated security products and procedures into their information systems. They also updated and tested contingency plans and backup facilities. We found that because of the staff training and industry testing that occurred around the century date change, employees of financial institutions and within our own agencies were still relatively well-informed about contingency procedures and arrangements, and followed them. Though not perfect, these plans worked well.

Third, financial institutions have long understood the need for strong internal controls and physical security. As banks increased reliance on information technology, they naturally incorporated measures to ensure the security of information. Moreover, financial institutions recognized immediately that the increasing role of information system networks and the Internet in the financial markets engendered new risks, and they became leaders in addressing cyberprotection issues. In 1999, industry participants established and funded one of the first information sharing and analysis centers (ISACs). More than forty of our largest banks, securities and insurance firms, investment companies, and financial utilities, representing a significant portion of assets in the financial system, participate in the ISAC. The ISAC maintains an industrywide database of electronic security threats, vulnerabilities, incidents, and solutions. Security specialists analyze reports and distribute to members warnings and information about threats and solutions or mitigation procedures. Financial institutions also actively participate in a number of other information-sharing organizations, such as the Federal Computer Incident Response Center (FedCIRC) and the System Administration, Networking, and Security Institute (SANS).

Fourth, supervisory expectations for business continuity planning and disaster recovery are long-standing. In general, the supervisory process focuses on a bank's risk-management and governance process, rather than mandating specific technical or operational standards. As institutions have expanded their use of integrated systems to support business operations, the potential for single points of failure has increased. In response, the banking supervisors have issued more detailed guidance on contingency planning, including managing information technology risk, information security, outsourcing, and network management. Examiners regularly assess the adequacy of business continuity plans. Moreover, the integration of information technology reviews into safety and soundness examinations and our evolving and expanding definition of the elements of operations risk are resulting in a more comprehensive approach to assessing the completeness and adequacy of business resumption plans.

Lessons learned from 9/11

Even when performing well in a crisis, one always has lessons to learn and to incorporate into one's planning. If we are to strengthen the overall resilience of the financial system, institutions will need to develop internal business-resumption standards and define their recovery targets in a fairly consistent manner. Decisions made by an individual institution may affect not only its own safety and soundness but also the safety and soundness of other institutions and, indeed, the very functioning of the financial markets. As a result, we believe that coordinated discussions about sound practices for business continuity involving industry participants and regulators are an important part of our response to the events of 9/11.

The Federal Reserve, along with several other financial regulators, met with a number of the larger financial firms in February to discuss how 9/11 has affected their thoughts about business-resumption planning. Our discussion group agreed that the focus of business continuity plans should be the smooth functioning of the financial system, particularly for firms that perform core functions in the wholesale and retail markets. Moreover, the group recognized, more keenly than before 9/11, the inter-dependence of financial system participants, wherever located. The group also agreed that planning assumptions about the scope and duration of operational disruptions need to be broadened. The group came to several other conclusions that I would like to highlight:

- Business resumption plans need to be expanded to provide for wide-scale and regional events. They also should take into account the loss or inaccessibility of staff.
- Obvious vulnerabilities are associated with the current geographic concentration of market participants and some of their backup facilities. As a result, geographic diversity for critical operations and backup facilities should be a key consideration of business-resumption plans.
- Institutions should identify their critical business lines and the systems or business processes that support those lines, including closely related activities that should have the same level of resiliency. They should also consider the extent to which their critical business lines depend on external parties--market utilities, major counterparties, and customers--and how to mitigate the risks that dependence poses for the continuity of operations.
- We must make certain that business continuity arrangements will be effective and compatible within and across institutions. The industry can accomplish this effectiveness and

compatibility only through developing multiple levels of backup, depending on the criticality of the function or business line. Moreover, our discussion group believed that industry participants must engage in robust testing of their contingency plans and backup facilities, internally and with financial utilities.

- Business-resumption plans should reflect recovery-time objectives for critical functions. Previous assumptions about how long backup facilities may need to be used and their capacity levels should be revised to incorporate the possibility of longer-term disruptions and to accommodate normal or increased volume of transactions--as occurred when the markets reopened on September 17.

The financial industry's dependence on telecommunications is well known, and 9/11 provided a vivid demonstration of how disruptions to the nation's critical infrastructure can and will close markets and disrupt payment flow. As you know, to ensure fair and orderly markets, the New York Stock Exchange, although it was fully operational, did not reopen until Monday, September 17, when voice and data links were restored. Although efforts are under way to improve the resilience of the telecommunications infrastructure, overcoming current vulnerabilities is clearly a long-term issue. For the time being, financial institutions should seek greater redundancy of telecommunications services through alternative technologies (Internet, satellite, and wireless) and eliminate potential single points of failure. I understand that, to obtain diversity in routing calls through wire lines, some firms are working with their telecommunications providers to document the routing of their telephone lines to obtain redundancy. However, this information is not always current or necessarily reliable. Moreover, because of the highly competitive nature of the telecommunications industry, competing providers have an incentive to concentrate and share facilities such as "switching hotels." That concentration may prove difficult to unwind without some fundamental change in the economics of the telecom market.

Implications for the financial institutions

Although, in practice, expectations for recovery times may differ depending on the scenario, some critical functions, including the safeguarding and transferring of funds and financial assets, are so vital to the domestic and global financial system that they arguably should continue with minimal, if any, disruption, even in the most severe regional disaster. Obviously, all institutions need to plan to continue serving customers in a major disruption, and supervisory standards have required them to do so for many years. However, it is increasingly evident that the operational resilience of the largest institutions in key markets should reflect their systemic impact across the financial sector. Expectations should be highest for institutions whose activity can significantly affect others, such as major clearing and settlement entities and institutions that act as financial "utilities" in some of their functions.

Our conversations with financial institutions and disaster-recovery experts indicate that some institutions are not just revamping emergency response and contingency plans to address vulnerabilities experienced during 9/11; they are considering some fairly significant changes in their operations.

For example, the traditional business-resumption model calls for having a backup for an active operating site, but maintaining an effective one is difficult. During 9/11, some firms found that their backup sites were not always accessible or that their backup systems did not have the up-to-date hardware and software versions in use at the active site. Some firms had only so-called "warm or cold" backup sites that required installation of hardware or software, which was not possible under the circumstances. Financial utilities, counterparties, and customers reported some difficulties in establishing communications because backup information had not been shared or was not current. Moreover, assumptions that key personnel could be relocated proved wrong. A variation of that business-resumption model includes shifting operations to the backup site on a regular basis. Doing so avoids the systems issues of the traditional model, but it still requires the movement of personnel.

Some institutions are moving toward a split-operations model in which two or more active sites provide backup for one another, and one site can absorb some or all of the critical work of the other for an extended time. Instituting this model may be easiest for institutions that have nationwide or global operations. The strategy offers the potential for an almost immediate resumption of business and addresses all the key vulnerabilities of the traditional model. At the same time, the split-operations model can involve significant costs in that it requires maintaining excess capacity at each site and

involves additional operating complexity to ensure a smooth shift of transaction and supporting data from one site to the other. I see this model as best suited for certain types of business activities that require as close to real-time information as possible, although I recognize that it dilutes internal synergy, which is particularly critical for trading operations.

As a result, firms need to balance all the competing factors in determining how to achieve an appropriately high degree of resilience for particular operations. Some functions may require more than one level of backup (for example, an active site with secondary hot and tertiary cold back up sites). At this point, activities that need real-time backup, such as the transferral of transaction information from a front office, are constrained geographically by existing technology. But the technology is rapidly evolving and, over time, will significantly expand the range of business-continuity strategies and change their relative costs and benefits.

The extensive interdependence among participants requires better coordination in identifying best practices and sharing information. Various trade associations (the Securities Industry Association, Banking Industry Technology Secretariat, and the New York-based Payment Risk Committee) have created industry-specific business-resumption work groups, and they are starting to meet. I trust that these coordination efforts will include the development of a plan for coordinated testing of backup sites by firms across the financial sector similar to the testing that took place in preparation for Y2K.

Initiatives by the Federal Reserve and Bank Supervisors to facilitate financial system resiliency

At the Federal Reserve, we are into evaluating and strengthening our business-resumption plans. As you may know, we were forced to evacuate the Federal Reserve Bank of New York for several days, and we relocated staff and operations to several backup sites. We are expanding our plans to ensure that critical central bank operations, supervisory functions, and financial products and services offices have sufficient redundancy in facilities and staff. One step that may be of particular interest is our plan to insure that if a Reserve Bank cannot operate, another Reserve Bank will be able to step in quickly to meet the discount needs of banks from the affected district.

As policymakers, we are evaluating our authority and flexibility in responding to situations that temporarily affect a bank's financial condition. I believe that our central bank tools were flexible and effective in providing the liquidity necessary to stabilize the markets in the days immediately after 9/11. We bought a record number of repurchase agreements, injecting approximately $81 billion into the government securities markets. We also loaned approximately $46 billion from the discount window--typical levels are around $100 million. And, to address the collateral needs of foreign financial institutions doing business in the United States and to meet the demand for dollars abroad, we executed a series of agreements to do currency swaps, if needed, with the European Central Bank, the Bank of England, and the Bank of Canada totaling $90 billion. The market reacted positively to the statements that we issued inviting banks to discuss with their regulators temporary balance-sheet issues arising from the market disruptions and encouraging banks to work with customers affected by 9/11.

The agencies also are busy at all levels updating emergency communication protocols and reviewing and improving strategies for communicating with financial institutions directly and with the public in times of crisis, when effective communication is particularly necessary. As we saw during 9/11, that being prepared and able to provide accurate and timely information to the public is critical to maintaining public confidence in the financial system.

Supervisors, in encouraging banks and other market participants to strengthen business-resumption plans, still have much to learn from financial institutions and experts in business-continuity planning. We have much less experience in modeling and predicting these operational risks than we have for understanding credit or market risk, and some threats may be too idiosyncratic to be modeled at all. Nevertheless, we are continuing our efforts to learn how financial institutions are applying the lessons they learned during 9/11 to their own business-resumption plans and are encouraging awareness and participation by senior management.

Our supervisory plans for the rest of the year and for 2003 are being revised to emphasize business resumption, particularly for large banking organizations. We are talking to institutions about the robustness of their contingency plans and encouraging them to ensure that the planning process includes participation from all relevant areas of their organization and includes expanded scenarios that take into account the effects that might flow from sudden, external events. But, we are stopping short of imposing detailed regulatory standards.

As best practices emerge to address the new paradigm, we may find it appropriate to expand supervisory guidance so as to obtain the appropriate level of overall resilience for the financial system. I expect we will come to some conclusion about the need for additional guidance over the next few months. However, I feel strongly that any such guidance should resist taking an overly prescriptive approach. Business resumption planning is not a "one size fits all" task. We want to encourage the industry to take advantage of rapidly evolving technologies and alternatives. In short, regulators need to balance competing issues. We have an important ongoing interest in the safety and soundness of individual institutions as well as in systemic financial stability. But we also recognize that, even though the largest nationally and internationally active institutions have a key role to play in financial stability, they also participate in a competitive marketplace. Thus, we need to be careful not to place undue burden on a handful of institutions. I expect that the marketplace will create its own incentives for institutions to invest in business resumption, as customers begin to demand assurances that their financial institutions can indeed continue to provide services if a regional or widespread operational disruption occurs.

Conclusion

Although these issues are complicated, we cannot afford to ignore the lessons learned from 9/11. As consensus emerges, we will have to expand our dialogue and encourage foreign financial systems, counterparties, and customers to seek levels of resilience necessary for the smooth operation of global financial markets. We have seen a sincere willingness on the part of industry participants to discuss business-resumption issues frankly and openly. I hope that industry members will incorporate best practices as appropriate to their particular business activities and in light of their role in the financial markets. We may have to prod a bit, but I am confident that, in the end, we will achieve an even higher degree of resilience for our financial system, which will be effective in responding to the panoply of imaginable--and even some unimaginable--events.