Summary of "Lessons Learned" and Implications for Business Continuity

February 13, 2002

Discussion note prepared by staffs of the Federal Reserve, the New York State Banking Department, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission, for discussion at a meeting on February 26, 2002 at the Federal Reserve Bank of New York

Summary

The Federal Reserve, the New York State Banking Department, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission have been jointly analyzing events in the wake of the September 11 terrorist attacks with a view toward strengthening the overall resilience of the financial system. This work has benefited from discussions with key members of the financial services industry over the past several months.

Insights from these discussions, which are summarized below, indicate that there may be significant benefits from developing more robust business continuity plans across the financial sector. Objectives of these enhanced plans could include:

- Rapid resumption of critical operations following the loss or inaccessibility of staff in at least one major operating location;
- Rapid resumption of critical operations following a wide-scale, regional disruption; and
- A high level of confidence (through ongoing use or robust testing) that critical internal and external continuity arrangements are effective and compatible.

The purpose of this discussion paper is to solicit views on the best way to develop and implement improved business continuity planning for the financial sector. The regulatory agencies referenced above are particularly interested in exploring the possibility of identifying and developing consensus on a set of "sound practices" that would embrace these, and possibly other, business continuity objectives; the range of firms and activities those sound practices should cover; and an appropriate method and timetable for their implementation.

I. Introduction

Despite the physical destruction, loss of life, and the widespread dislocations to financial institutions' physical operations and personnel resulting from the terrorist attacks on the World Trade Center in New York City on September 11, 2001, the U.S. financial system continued to

perform its vital economic functions. In an effort to ascertain the key lessons from this experience and to identify steps that could further strengthen the operational resilience of the financial system, staff of the Federal Reserve, the New York State Banking Department, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission have met with a number of financial institutions over recent months. There is a significant public interest in ensuring that, in the event of a large-scale disaster or disruption of natural or human cause, systemic disruptions to the banking and payment systems and financial markets are minimized, and that companies, consumers, and investors have confidence in their ability to effect transactions and access their funds, securities, and other financial assets.

The impact of the events of September 11 highlighted the interdependencies within the financial system, especially within the clearing and settlement infrastructure. It was clear that decisions made by key institutions regarding their individual level of preparedness for disasters or other crises significantly affected others, both directly and indirectly. As a result, a coordinated approach to enhanced business continuity planning appears to be needed to apply fully the lessons learned from September 11.

II. The Impact of the Events of September 11

During the week of September 11, the widespread destruction of physical infrastructure supporting financial institutions in and around the World Trade Center and extensive telecommunications breakdowns throughout the region caused dislocations in financial markets. U.S. equity markets were closed for four days and most bond trading, including government securities trading, halted for two days. There were significant disruptions in the clearing and settlement mechanisms for government securities, repurchase agreements, and commercial paper.

Although the core payments systems continued to work well, operational failures and telecommunications breakdowns among major financial institutions led to significant liquidity bottlenecks for several days. During this period, the Federal Reserve and other major payment systems remained open well past their normal closing times to accommodate institutions that were attempting to send funds or waiting to receive funds from other institutions. A number of institutions borrowed from the central bank discount window in substantial amounts to obtain sufficient liquidity to continue meeting their obligations. Other institutions and their customers built up high cash balances or held on to government securities positions for precautionary reasons, exacerbating market liquidity imbalances.

Some institutions could not ascertain their own financial positions or those of their customers for several days. Various prudential regulatory requirements were relaxed in the face of credit and liquidity disruptions and unreconciled transactions that caused significant, though temporary, balance sheet distortions across a wide range of institutions. Some transactions were lost and had to be reconstructed, a laborious and inexact process. Vaults containing physical certificates were destroyed and records identifying these certificates were not always readily available. Reconciliation of disrupted transactions continues to this day.

At the same time, the extraordinary levels of cooperation by market participants in the aftermath of the September 11 events helped overcome limitations within the scope of firms' business continuity planning. Some firms were accommodated by other organizations (including competitors) in the New York City area in finding office space for staff. Customers and counterparties helped re-create transaction records that were lost. Institutions extended credit to customers and counterparties hampered by liquidity shortfalls despite the inherent uncertainty and lack of reliable information in the marketplace about their current financial condition. Large numbers of people inside and outside the financial industry worked long hours to restore communications links that had failed. In fact, the most oft-cited lesson learned from the tragedy is the importance of people, including considerations for their personal safety as well as their dedication and critical role in keeping institutions functioning in times of crisis.

III. Major Vulnerabilities

The systemic effects highlighted several important vulnerabilities that may not have been widely appreciated prior to September 11. First, it was clear that business continuity planning had not fully taken into account the potential for wide-area disasters and for major loss or inaccessibility of critical staff. Contingency planning at many institutions generally focused on problems with a single building or system. Some firms arranged for their backup facilities to be in nearby buildings on the assumption that, for example, a fire might incapacitate or destroy a single facility. Very few planned for an emergency disrupting an entire business district, city, or region. As a result, some firms lost access to both their primary and backup facilities in the aftermath of the September 11 events, severely disrupting their operations. Institutions also generally had not considered the possibility that transportation of personnel could be significantly disrupted and preclude the relocation of staff to alternate sites.

Second, concentrations, both market-based and geographic, intensified the impact of operational disruptions. Financial institutions are significantly concentrated within the geographic area in New York City most affected by the devastation at the World Trade Center; indeed, over recent years, some institutions have consolidated their staff in one or two locations for efficiency purposes. In addition, some critical market functions, particularly in the clearing and settlement of funds, securities, and financial contracts, rely on a small number of entities with operations in a concentrated area. In addition, significant vulnerabilities in telecommunications capabilities resulting from concentrations became evident when telecommunications failures affected numerous institutions, including backup as well as primary sites in the same region. Many firms believed they had achieved redundancy in their communications systems by making arrangements with multiple telecommunications providers or by contracting for diverse routing, only to discover that all of the lines traveled through any of several now well-known single points of failure.

Third, the events of September 11 graphically demonstrated the interdependence among financial system participants, wherever located. While organizations located outside the New York City area were affected to a much lesser degree than were those within it, many felt the effects of the disaster. Most lost connectivity to banks, broker-dealers and other organizations in lower Manhattan, which impeded their ability to conduct business and determine whether transactions

had been completed as expected. Some customers were affected by actions of institutions with which they did not even do business, when funds or securities could not be delivered due to operational problems at other institutions.

IV. Business Continuity Models

The events of September 11 may lead to changes in the way that institutions plan for emergencies, as well as changes in their ongoing operations. It is helpful to review the basic models for business continuity planning and how these fared during the recent crisis.

A. Traditional Active/Backup Model

In its simplest form, the traditional model of business continuity is based on an "active" operating site with a corresponding backup site, both for data processing and for operations. This strategy generally relies on relocating staff from the active site to the backup site, and on maintaining backup copies of technology and data. There is an inherent dependency on the staff at the active site and their ability to move to the backup site. An adequate "desktop" recovery strategy – one that contemplates the movement of, at a minimum, core employees to fully functional backup office space – is a critical element of this model. This approach tends to limit geographic separation to reduce relocation time. Common approaches for the backup of technology infrastructure and data processing also rely on keeping data, hardware, and software current at the backup site and on resilient and diverse services (including telecommunications and electric power) at each site.

While the traditional active/backup model has been considered cost-effective and practical for many purposes, this model creates internal and industry-wide challenges to ensure that the combinations of primary and backup sites across diverse counterparties are compatible, well understood by all relevant parties, and have up-to-date technology and procedures. In the traditional model, backup capabilities are generally assured through planning and testing. Even with regular testing, it is often difficult to maintain the effectiveness of backup sites, staff, and systems that are not routinely used for production purposes. For example, during the week of September 11, many institutions found that disaster recovery plans of particular business lines were not always accessible or up-to-date.[1]

Other vulnerabilities of the traditional model were evident during the week of September 11. Some firms – particularly smaller ones – sent records offsite only at daily or weekly intervals. As a result, when they lost their primary offices, they had to devote substantial resources to reconstruct records that had not yet been transferred to their backup facilities. The experience also suggested that recovering critical real-time processing operations from backup tapes is generally not realistic for large institutions' or for critical high-volume processing activities. Most larger institutions now employ data "mirroring" or remote real-time transaction logging technologies through which transactions are transmitted immediately to a second (and in some cases, third) site. However, even in some of those cases, problems such as out-of-date software, reduced systems capacity, and inadequate telecommunications at the backup site often were not

[1] Institutions are moving toward maintenance of disaster recovery plans for each business unit or other operating level in a centralized database that is accessible from multiple locations. A centralized database also facilitates oversight and consistency of individual plans and testing activities.

discovered until operations were in the process of being recovered. In addition, not all institutions had made adequate back-up arrangements for all critical supporting systems, such as the operating "front-end" (i.e., those systems, networks, and processes providing interface with customers, counterparties, and clearing and settlement utilities).

Institutions using the active/backup model also may rely on the services of a third-party to provide the backup facilities. Many financial institutions, particularly smaller ones, have contracted with third-party disaster recovery vendors for backup space for staff or computers. During the days following September 11, some disaster recovery vendors found they were unable to accommodate all of their affected clients, with the result that several institutions found themselves without the anticipated backup facilities. Moreover, the very small number of disaster recovery vendor sites supporting a large number of major financial institutions across the country may represent another vulnerability.

B. Split Operations Model

An emerging business model, which is used by some firms with nationwide or global operations, is to operate with two or more widely separated active sites ("active/active") for critical operations that provide inherent backup for one another. For banking organizations with nationwide operations, for example, such sites are often hundreds of miles apart. For international firms, routine workloads can be shared among sites in different countries. Each site has the capacity to absorb some or all of the work of another for an extended period of time. This strategy can provide close-to-immediate resumption capacity, depending on the systems used to support the operations and the operating capacity at each site. This strategy addresses many of the key vulnerabilities noted above, eliminating dependency on availability and relocation of staff at any single location, reducing likelihood of telecommunications single points of failure, supporting maximum geographic separation, and assuring business continuity through actual use, rather than infrequent and less than complete testing.

At the same time, the split-operations approach can have significant costs, in terms of maintaining excess capacity at each site and added operating complexity. Depending on the sophistication of the function involved, it also may be impractical to maintain appropriately trained staff at multiple remote sites. After the World Trade Center attacks, some firms with offices in other U.S. cities or overseas redirected some limited trading and sales activities to those locations as a stop-gap measure. Although in some cases, this arrangement worked well, in others, the remote offices lacked sufficient personnel trained to perform these functions, or to perform them at the required capacity.

Even with the active/active model, current technological limitations also preclude wide separation of data centers that use fully real-time, synchronous data mirroring backup technologies. However, other technologies are in use by some institutions that permit much more distant replication of data at multiple sites, so long as some slight time lag between sites can be tolerated by the institution's business. As technology advances and other techniques become more robust, greater geographic diversification of technology operations may very well become practical for many firms.

C. Other Models

There may be other business continuity models that can provide a high degree of resiliency. For example, some institutions employ a variation on the above models in which a backup site periodically functions as the primary site for some period of time ("alternate site" model).

In addition, it is important to recognize that these models are not static, and to consider how technological change may affect the choice of business continuity models and methodologies over time. For example, the September 11 events demonstrated that business continuity is enhanced where records are kept electronically, allowing even the most current records to be replicated and recovered at backup sites. In addition, some institutions have noted that by increasing automated processing, backup arrangements are more straightforward, as they do not depend as much on large-scale staff relocation. For some institutions and their customers, recent events including the grounding of air transport and disruptions of mail delivery, are prompting further movement away from physical, paper-based transactions and recordkeeping systems in favor of electronic methods. Nonetheless, although electronic records help protect against loss of a physical site, dependence on electronic records increases vulnerability to cyberattacks and to defects in hardware and software.

V. Developing Sound Practices for Business Continuity

In the face of revised assessments of the types, severity, and probability of potential threats, the cost-benefit balance of enhancing resilience to these threats has clearly shifted post-September 11. There are a number of steps, described below, that may help achieve a common view of sound practices for business continuity.

A. Define the Scope of Scenarios

A core question is the range of scenarios that financial institutions realistically need to address in their business continuity planning. There are a number of scenarios that would affect particular geographic areas, such as explosive devices, biohazards, and natural disasters. Such scenarios could render a large area inaccessible and could harm or disperse an organization's critical employees. Other scenarios might deal with cyberterrorism, which is aimed at computer networks and systems, rather than a particular physical location, although this threat is the focus of other efforts within the public and private sectors and is not addressed here. Scenarios may also need to encompass targeted attacks on a key element or elements of the financial system.

In light of the September 11 experience, most now believe that the financial services industry must consider how to achieve greater geographic diversity of operations among major financial institutions and clearing and settlement providers in order to withstand events of greater geographic scope than previously considered. Many now see the need to plan for extended periods of inaccessibility of more than one operating site within the same area. City-wide disruptions may be the minimum benchmark for planning purposes going forward, and the ability to withstand disruption of an entire metropolitan area or region is also being considered by some organizations.

Expectations have also changed regarding the length of time an event may incapacitate an area, which has implications for the depth of business continuity planning. For example, institutions whose operations or data centers were destroyed or rendered unusable in the World Trade Center attack were often left operating at a backup site indefinitely, without adequate backup for that site. Accordingly, the most critical elements of the financial system may need to consider some additional level of backup, such as a tertiary site that can take over processing or serve as a backup if primary or secondary sites are unusable.

B. Establish Business Continuity Objectives

Business continuity objectives or principles need to be articulated that are consistent with cost-effective, sound business operations and that take into account the impact that one critical institution's operations can have on another. These objectives could cover issues such as:

- Recovery time expectations for critical operations.
- Recovery capacity or volume expectations.
- Sound business continuity practices to support these objectives.

Although in practice, recovery time expectations may differ depending on the scenario (e.g., the expected times for institutions to recover from a localized power outage may differ from that of a regional disaster with loss of life), there are critical functions, including those relating to safeguarding and transferring of funds and financial assets that are so vital to the U.S. and global financial system that they arguably should continue with minimal, if any, disruption even in the event of a major regional disaster. The near-immediate "fail-over" capabilities provided by current technologies can support this objective. The events of September 11 demonstrated that institutions that had planned for and tested their ability to recover critical processing operations at least within the business day fared significantly better in resuming normal operations.

Additionally, recovery objectives with respect to operating capacity may need to be reassessed. Many institutions' backup arrangements were based on plans to handle a reduced volume of activity during a disaster scenario. In fact, Monday, September 17, was an exceptionally high volume trading day, and the shifting of settlement timeframes for government securities led to wide fluctuations in day-to-day settlement volumes. Some institutions found that systems and telecommunications backup lines were designed to operate at significantly lower volume, severely hampering their ability to complete all processing during the disaster.

C. Identify Key Elements of the Financial System

A coordinated industry-wide approach to business continuity planning requires identification of the critical operational components of the financial system that must achieve a high level of business continuity preparedness. A primary question is whether and how business continuity objectives should differ for institutions or infrastructure components with different levels of systemic importance. In particular, expectations may be highest for institutions whose activity has the potential to significantly affect other institutions, such as major clearing and settlement

entities, as well as institutions that essentially act as financial "utilities" in some of their functions. Other institutions may be collectively critical to the daily operations of financial system, but individually of less systemic significance.

It is also useful to identify the types of operations that may require the highest level of operational resilience for major financial institutions. This may involve identification of the core markets (e.g., money markets, government securities, foreign exchange, commercial paper, equities, derivatives) and essential functions supporting these markets (e.g., trading, brokering, transaction execution, clearing, settlement, custody, customer contact).

Sound practices for the financial sector necessarily include planning with non-financial institutions, such as telecommunications utilities and other vendors of various infrastructure services. Institutions are already exploring methods to provide greater assurance that diversity of telecommunications lines is achieved and single points of failure are eliminated. Contract provisions and audit oversight may help heighten attention to this critical vulnerability. At the same time, many recognize that overcoming telecommunications vulnerabilities will be extremely difficult given the current physical infrastructure. Establishing diverse telecommunications methods and moving toward wider geographic diversification of operations in the longer term may be more effective in addressing these vulnerabilities. Disaster recovery vendor arrangements are also being reexamined by some institutions.[2]

D. Testing and Crisis Management

Finally, the effectiveness of common business continuity strategies needs to be assured, whether through planning and testing or through regular use. Some institutions found that their routine testing of their business continuity plans as frequently as monthly or quarterly helped considerably in dealing with the crisis, relative to annual or less frequent testing. While testing and planning absorbs resources, institutions have found ways to integrate business continuity tests into their routine operations, such as by actively switching live operations to alternate sites periodically.

The events of September 11 demonstrated that business continuity plans, procedures, and testing need to reflect internal interdependencies, such as between payments, custody, funding, trading, and issuing/paying agency functions, as well as external dependencies and relationships. In addition to operational and safety decisions, financial institutions need to make credit and market risk judgments with respect to customers and counterparties, whose financial condition may not be certain during a crisis.

Coordinated testing of business continuity plans between institutions and their customers or counterparties has not been a common industry practice, but some have observed that joint testing exercises may be needed going forward. While most firms had conducted some testing from their backup sites, the tests generally were with the primary sites of customers and the

[2] For example, one approach being explored is the use of exclusion zones, whereby disaster recovery vendors do not contract the same space to any institution within close proximity of another that has contracted for the same space for use in a disaster.

clearing and settlement utilities. In the wake of the September 11 disaster, many market participants found themselves operating from their backup sites and discovered connectivity and other communications problems to the backup sites of other displaced entities. The industry may need to explore whether some degree of coordinated testing between backup facilities of key market participants could help in addressing operational interdependencies across institutions and utilities.[3]

Many institutions found that their sound business continuity planning and testing helped significantly on September 11 in locating and communicating with staff during the initial hours of the crisis, making key financial and operational decisions, and quickly restoring relatively normal operations. The importance of accurate and clear information flows, both internally and externally, was particularly evident during the week of September 11. During a crisis, proactive, ongoing, and honest communication regarding operational status to customers, counterparties, and regulators can help others to make informed decisions and avoid exacerbating credit and funding dislocations.

In addition, many institutions have noted the need for the industry to consider whether a more coordinated approach to crisis management and communication needs to be developed. Since September 11, several public and private-sector initiatives have begun to address the issue of coordinated crisis management communication within the industry and with regulators.

VI. Discussion Questions

Initial discussions among financial institutions and regulators suggest that institutions are aware of the most important vulnerabilities described above. Most firms appear ready to commit the necessary resources to strengthen the resilience of the industry as a whole, particularly if similar institutions adhere to similar standards. Industry and regulatory consensus on these standards will increase the likelihood that all institutions will make individual planning and investment decisions that are commensurate with their role in the financial system and that reflect the interdependencies that permeate the financial system.

As a result, the regulatory agencies would like to explore the feasibility of developing a common set of sound practices embodying highly resilient business continuity objectives. Industry input on several key questions will be needed in this process:

1. For what range of scenarios should the financial sector be expected to plan?

As noted above, there is a growing consensus that the industry must plan for events of wider geographic scope and greater physical disruption than in the past, including those that involve loss or inaccessibility of critical staff or of widespread telecommunications or other services disruptions. City-wide disruptions may be the benchmark for planning purposes going forward, and regional disruptions also need to be considered.

[3] Informal discussions regarding coordinated testing have already begun among the major payment utilities.

2. What are appropriate sound practices for business continuity planning that support common recovery objectives, in light of these scenarios?

Sound practices should provide for very rapid resumption of critical operations at stressed volumes of activity following a wide-scale, regional disruption that could result in loss or inaccessibility of staff in at least one major operating area. Industry consensus at this stage on these, and potentially other high-level recovery objectives would help guide the work that will be required to develop common sound practices that are sufficiently detailed to be meaningfully applied, yet accommodate a range of operations models and ongoing technological change.

3. How broadly should the sound practices be applied?

Regulatory and supervisory requirements generally set out minimum standards applicable to a range of different institutions. Clearly, the major financial institutions collectively need to plan for very robust business continuity objectives for the essential functions they provide in support of core markets. In addition, the level of business continuity planning and investments made by the largest or most critical firms in some activities may have consequences for other institutions. Industry guidance is sought on whether the nature of the recovery objectives and associated sound practices may need to differ depending on the systemic importance of the institution and activity. If so, decisions would need to be made on which entities and activities would fall into the "top tier." For example, some have observed that clearing and settlement utilities and institutions providing similar services should be expected to meet the highest standards or recovery objectives.

4. What is the best way to develop and implement these sound practices?

Input from the financial sector is essential to determine the most effective way to ensure that common sound practices are implemented as widely and as quickly as possible. There may very well be a need for supervisory and regulatory standards to support the application of sound practices across the industry. The industry may also be able to provide guidance on how to provide a high level of confidence, through ongoing use or robust testing (including coordinated testing), that the plans implemented by individual institutions are effective and compatible across the industry.