A REPORT TO THE INDUSTRY ON BUSINESS CONTINUITY PLANNING

Safe, Secure, Setting New Standards

DTCC.

The Depository Trust & Clearing Corporation

Safe,
Secure,
Setting New Standards

An Updated Report to the Industry on Business Continuity Planning.

July 2011

Safe, Secure, Setting New Standards

An Updated Report to the Industry on Business Continuity Planning.

Table of Contents

Executive Summary

Since the events of September 11, 2001, the need to protect the global financial system has brought heightened attention to business continuity planning, both in the United States and in markets worldwide. The need is particularly acute for The Depository Trust & Clearing Corporation (DTCC), the largest post-trade financial services infrastructure company in the world. Safeguarding DTCC's ability to support its critical clearing, settlement and asset servicing roles, as well as the highly specialized knowledge of its employees, is acknowledged by the industry and regulators alike to be essential to sustaining the safety and soundness of U.S. financial markets.

Contingency and continuity planning goes back many years at DTCC. Over the past several years, however, DTCC has moved aggressively—as have other companies in the industry—to upgrade its continuity plans and expand its resources in order to strengthen the resiliency of its business operations against the possibility of wide-scale disruption. DTCC continues to be a leader in the securities industry in the efficiency and effectiveness of its business continuity planning and facilities. DTCC's own resiliency, however, is only part of the story. The resiliency of DTCC's industry partners and participants, and of key infrastructures on which all of us rely, is equally important to assuring the ability of the financial markets to continue in the face of extreme events. Recognizing this, we believe it is important to share DTCC's experience and the practical knowledge it has gained to encourage wider and more informed discussion and focus on business continuity planning throughout the industry.

The purpose of this report is to contribute to and continue that dialogue by reviewing how DTCC has approached various business continuity issues, what we have learned about them, and how we have modified our plans through these experiences. We hope that this will help our participants and others in the market in their own thinking about these problems. Specifically, this report seeks to:

- Spell out the challenges we anticipate and plan for at DTCC;
- Discuss the reasons we have taken a leadership role in business continuity planning;
- Document the steps DTCC has taken so far to help ensure safety and soundness in U.S. financial markets;
- Assure the financial services industry and government agencies that we intend to maintain our leadership role;
- Alert our customers and participants that we will continue to conduct planning exercises and connectivity tests, and that network changes we are planning to ensure greater centralized control and resiliency may require their participation; and
- Encourage more discussion about continuity planning as a way to help advance the further development of industry best practices.

Building on our existing continuity plans and drawing on our experience and that of the industry during 9/11 and the 2003 blackout in the Midwest and Northeast, we have developed—and tested—action plans for each of the key challenges facing DTCC. We now have plans and resources in place to:

- Achieve recovery, even in the most dire circumstances, within the two-hour window mandated by government agencies, with faster recovery the objective in less extreme situations.
- Increase employee safety and disperse staff across geographically diverse operating facilities in accordance with the recommendations of an interagency government paper.
- Operate multiple back-up data centers linked by our highly resilient network technology.
- Provide tighter emergency command and out-of-region operating control.
- Utilize new technology we developed in conjunction with partners to provide high-volume, high-speed, asynchronous data transfer over distances of 1,000 miles or more.
- Reinforce our processes that mitigate marketplace, operational and cyber-attack risks.
- Test our own continuity plan readiness and connectivity on a regular basis, ensuring that our customers can connect to our primary and back-up sites and that we can connect to their primary and back-up sites.
- Communicate on an emergency basis with the market, our customers and government agency decision-makers.
- Evaluate, test and utilize best business continuity and resiliency practices.

There are, of course, limits to the information about our plans and facilities that we can share with the public. In fact, some of the information and discussion in this report has been purposefully cloaked to maintain security. But we are confident the report can achieve its purpose without disclosing any information that would compromise the security of DTCC's employees, plans or facilities—or those of any other industry participant.

Questions, comments or queries should be directed to Messrs. George Perretti, DTCC Managing Director, Corporate Business Continuity telephone - 212 855-8176, e-mail - gperretti@dtcc.com; or Ken Wright, DTCC Director, Corporate Business Continuity, telephone - 212 855-1368, e-mail – kwright@dtcc.com. Additional contacts for various specific elements of DTCC's contingency planning are listed in the appropriate sections of this report.

Overview: challenges and responses

The overriding industry challenge

One of the most critical challenges facing the global financial services industry is to ensure rock-solid resiliency and sufficient redundancy in the industry's infrastructures to guarantee the continuity of clearance, settlement and asset servicing in the event of a disaster or widespread disruption affecting one or more critical financial markets. In the aftermath of 9/11, for example, the collapse of communication links in sections of New York City impacted a key services provider to the U.S. government securities markets, causing a multibillion-dollar clearing backlog. That, in turn, resulted in severe, although temporary, liquidity problems for a number of market participants. The interdependent nature of financial markets means that, without sufficient resiliency to withstand disruptions, there could be *systemic* repercussions reverberating across critical market structures--and hence the markets themselves.

In response to this profound systemic issue, U.S. financial regulatory authorities issued an *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*[i] in 2003. The paper identifies three business continuity objectives that have special importance for all financial firms. They are:

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

Papers and documents on business continuity released by other authorities – both regulators and industry groups such as the Group of Thirty[ii] – all agree on these key objectives.

The DTCC challenge

Just how rapid an organization's "recovery and timely resumption of critical operations" should be necessarily depends on the role the organization plays in the financial services industry. For core clearing and settlement organizations such as DTCC, there is general agreement among regulators and industry participants (at least within the United States) that the goal for "within-the-business-day" recovery and timely resumption of critical operations should be no more than two hours from the time of dislocation. DTCC's contingency plans are geared to achieving such a rapid recovery even in the direst circumstances, with faster recovery the objective in less extreme situations.

DTCC has accepted the challenge of meeting this very rigorous standard for recovery because, as the largest post-trade financial services infrastructure organization in the world, we have a central role in the functioning of the capital markets. Through its subsidiaries DTCC provides clearing, settlement and information services for virtually all trades in U.S. markets, including trades in equities, corporate, municipal and government bonds, mortgage-backed securities and the broad array of money market instruments. In 2010, DTCC's subsidiaries

cleared or settled transactions valued at USD 1.66 quadrillion. This translates into approximately $6.6 trillion worth of transactions processed each business day in 2010. In other words, DTCC settles securities transactions roughly the equivalent of the entire U.S. gross domestic product every two days. On average, DTCC's clearing corporation clears 81.5 million equity "sides" a day with a value of almost USD 870 billion. DTCC's depository maintains custody of more than 3.6 million securities issues, including instruments issued by companies and governments in more than 121 different countries.

An extended delay in carrying out these activities could create operational, financial and structural problems for market participants that would readily spill over into the markets themselves. For example, since DTCC's clearing subsidiaries take on counterparty credit risk in the clearing process for many securities trades, they assume trillions of dollars worth of credit risk on behalf of their participants each day. A failure of clearing corporation operations would, at minimum, introduce unprecedented uncertainty into the markets, if not forcing them to temporarily suspend operations. In the same way, a failure in the data processing or communications systems that DTCC's depository subsidiary uses to settle trades could leave millions of market transactions uncompleted, sowing confusion among market participants and stretching intra-day credit facilities. Events of this magnitude could halt investment activity in most U.S. securities for an uncertain period, devastating investor confidence in the financial markets. Because U.S. and foreign markets are interdependent and foreign investment in the U.S. markets is substantial, a cataclysmic event affecting the U.S. financial system could also have implications worldwide. DTCC has no choice but to ensure that its systems and operations meet the highest standards of resiliency.

The DTCC experience: testing plans and validating assumptions

Along with many other financial services companies, DTCC brings hard-won experience to continuity planning. At DTCC, continuity planning has always been an integral part of our business culture. For more than a decade, DTCC has had in place back-up data processing operations providing for multi-center control of data processing operations and the synchronous/asynchronous replication of critical participant data to multiple sites. For more than a decade, each of the company's operating units has been required to draw up detailed recovery plans and test them regularly. These are some of the key reasons DTCC succeeded in keeping all of its critical services fully operational on 9/11 and in the week that followed, allowing the company to settle outstanding transactions valued at more than USD 1.8 trillion.

The events of September 11th, however, made clear to us and to all in the financial services industry that we were operating under a new paradigm. No longer could we simply plan to maintain business continuity in the face of localized problems such as a severe storm, a fire or a flood. We now had to plan for previously unthinkable or unimaginable scenarios with potential repercussions across an entire region or financial market--or beyond.

Within two weeks of 9/11, DTCC had already begun a rigorous review of its disaster recovery and business continuity plans in order to identify strengths and weaknesses in the context of this new understanding of business continuity and to build on the experience gained. In addition to examining our actions and responses, we assessed which continuity systems and operating

procedures worked well and which did not, the kinds of problems our staff encountered, the various challenges our customers had to cope with, the banking and payment issues that emerged, and the points of vulnerability, such as communications, that became apparent across the market. While this analysis identified what had been learned from the actual experiences of the days following the September 11th attacks, its primary focus was on evaluating whether the security and business continuity plans we then had in place would be sufficient to address those new potential vulnerabilities and threats that could play a role in future disruptions. The results of this analysis, and the steps DTCC has taken in response to issues it identified, have been in part shared with the industry over the past several years, and are further described throughout this paper.

Subsequent experience gained in the power blackout of August 14-15, 2003, the most severe in U.S. history, also proved valuable—and affirmed some of the conclusions we had drawn in our immediate post-9/11 analysis. In fact, the blackout afforded a good test of DTCC's new contingency procedures. Again, DTCC remained fully operational, handling normal clearing, settlement and asset servicing activities. We transferred lead responsibility for business operations to one of the company's remote operating locations, while the command center in another of the company's remote facilities—unaffected by the blackout—stepped in to manage data processing operations. As it routinely does in such emergencies, DTCC also began contacting its customers to make sure they would be capable of conducting settlement, while company executives consulted throughout the night with industry, regulatory and government organizations to ensure that preparations were complete to permit smooth clearing and settlement operations on day two of the blackout. Additionally, to reassure the financial markets and its customers in the United States and abroad, DTCC put out a public statement that settlement of securities transactions would be completed as usual.

DTCC is also convinced that a key part of the industry's overall response to the business continuity issue is the pressing need to streamline and accelerate business procedures. The less convoluted and more direct industry processes are, the easier they are to maintain under difficult circumstances and the more quickly they can be restarted if stopped. This is a key reason—in addition to the greater efficiency we achieve—that we work to apply straight-through processing (STP) wherever we can. For example, the implementation of real-time trade reporting from the major equity marketplaces and the Real-Time Trade Matching (RTTM) service for fixed-income securities allow us to capture and record data on trades as they take place, rather than minutes or even hours later. The capture and movement of the data to our systems on a straight-through basis minimizes the likelihood of a data loss. Had RTTM been in place on 9/11, for example, it would have been much easier for firms evacuated from their offices to recover trading records and avoid the snowballing confusion about inventory positions and the status of trades that followed this catastrophic event. Meeting the challenge of business continuity includes placing a high priority on industry STP initiatives.

Over the last few years, DTCC has developed and implemented action plans to deal with the challenges noted above. We completed and implemented some of the planning initiatives well ahead of industry and government timetables. Others, while operational, are undergoing additional development. In our role as a leader in business continuity planning, we continue to look for and try to cull best practices from throughout our own industry and, where applicable, other industries.

Implementing, advocating and redefining business continuity best practices on multiple fronts

1. Protecting People and Sustaining Business Operations

DTCC shares the view of many industry leaders that concern for the safety and security of the people who work in the financial services industry must be the number-one priority. The continued ability of the industry to meet the financial needs of investors in the United States and around the globe is critically dependent on its people, and DTCC's ability to help the industry meet those needs is critically dependent on DTCC's employees. Consequently, DTCC regards the safety and security of its employees as the highest priority objective of its infrastructure protection efforts. Without our staff, we cannot deliver the resiliency and assured continuity of business operations that the industry and investors everywhere expect. We have reinforced emergency procedures at each of DTCC's locations and practice them on an ongoing basis. In addition, to gain knowledge of best practices, we continue to examine the practices and operating procedures of other companies in the industry.

Staff Decentralization – To address the concentration of critical expertise or knowledge capital of our employees, DTCC's staff has been decentralized to a degree not previously seen. We possess critical operating capacity in multiple locations and have similarly redistributed technology staff and other key functions. In addition, we have relocated a portion of DTCC's relationship management staff away from headquarters to ensure an ongoing ability to interact with customers in the event of an emergency. To facilitate this decentralization, DTCC has expanded the capabilities at its remote data center to include additional staff and implemented an out-of-region Operations center (the Southern Business Center, or SBC) for business operations in 2004. SBC was fully staffed and operational during 2005. Doing so involved relocating a substantial number of tenured employees, augmented them with hires from the local marketplace and mirrors the thinking in the federal government's interagency white paper, which requires stronger measures to ensure recovery from a widespread regional disaster. The interagency paper says that ―core clearing and settlement organizations . . . whose back-up sites depend primarily on the same labor pool as the primary site should address the risk that a wide-scale disruption could impact *either or both of the sites and their labor pools* (emphasis added). Such organizations should establish even more distant back-up arrangements…. The staff decentralization at the Southern Business Center addresses this concern and eliminates the risk associated with the former staffing model.

Communications are critical in an emergency—particularly staff communications. We deploy various means of staying in touch with staff during emergencies. These include public address systems at all locations which permit DTCC senior executives to speak directly to the staff in emergency situations, an employee telephone hotline with up-to-the-minute information, a telephone service that allows us to deliver messages to specific groups of employees, the capability to broadcast e-mail to employees and message centers on DTCC's Internet sites. Employee contact information and responsibilities for calling employees in particular operating

units are also embedded in "calling trees." Every DTCC unit must maintain and periodically update its calling trees.

Priority phone service and emergency access - Twice a year senior managers receive wallet cards with updated contact numbers (home phones, cell phones and pager numbers) for the top levels of management and other critical contacts. Critical employees are also equipped with cell phones, pagers, Blackberry communicators and other devices. In addition, DTCC has arranged to have senior managers covered under the U.S. government's Government Emergency Telecommunications Service (the "GETS" program) and (WPS) Wireless Priority Service. This gives card holders access to the U.S. government's emergency telephone priority service for both land lines and cellular devices. The City of New York also has implemented its Corporate Emergency Access System (the "CEAS" program), which permits certain personnel access to areas that have been restricted in the event of an emergency. DTCC senior executives and critical staff participate in the CEAS program.

Employee safety is DTCC's primary focus in an emergency and a sweeping program has been put in place to address training and procedures for employees. The company's emergency response plan also includes evacuation procedures and points of assembly for each operating facility.

- Employees also practice evacuation procedures several times during the year. Since some of DTCC's locations are in multi-tenant buildings, DTCC's own evacuation drills provide only a partial test of what an actual evacuation would be like (because in an actual situation other building tenants would also be evacuating). To identify any issues that could come up in such a situation, DTCC is currently in discussion with other tenants in certain of its locations on conducting tests involving a total building evacuation.
- Maps have been posted on all floors in all DTCC locations, and included in employee emergency guides, identifying the "points of assembly" to be used in the event of a building evacuation. The map on a particular floor identifies the assembly point for the staff on that floor.
- DTCC staff members have been given "safety kits," with safety equipment and devices (such as an anti-dust breathing mask) to be used in an emergency situation. DTCC had outfitted its staff with similar safety kits prior to September 11th, and many employees found them very helpful on the day of the attacks.

Physical security remains a top priority. As a matter of practice, DTCC has always maintained strong physical security measures for its premises. Over the last several years, we have further enhanced our security program to include coordinating efforts with the building management at each of DTCC's various locations to strengthen protections in these buildings. At our headquarters building, for example, heavy concrete planters and bollards were installed to provide protection against a physical attack on the building perimeter. Tenant identification is rigorously checked at building entrances, and an X-ray machine and a magnetometer are utilized to screen visitors for weapons or explosives. A security canine team periodically checks building perimeters and, in our message centers, all packages are screened via X-ray. A "blast room" is used to screen all incoming mail. We also coordinate our security activities closely with local law enforcement as well as with federal authorities.

2. Ensuring Certainty of Data and Systems

Create multiple, geographically dispersed facilities to ensure system redundancy and data safekeeping

In addition to its headquarters facilities, DTCC now has operations and staff in multiple locations elsewhere in North America. All of DTCC's data processing locations are now fully operational, all support data replication and disaster recovery capabilities, and DTCC can conduct all critical systems functions from any location.

Geographically dispersed back-up facilities – Not only does DTCC now have operations and staff in multiple locations, including sites outside the New York City area, but those locations, including remote data centers, are fully operational. If a major disaster were to destroy or cut off DTCC's New York region data processing locations, DTCC would still be able to resume critical data processing operations including all key depository functions and key clearing functions. We can use any center if our primary work sites are not accessible or operable. Likewise, we can conduct all critical systems functions supporting DTCC's delivery of its clearance, settlement, income processing and corporate actions services from these various locations. All sites have the computer capacity for total data replication and are linked to DTCC's SMART network. (See a more detailed description of SMART under the Network Technology section below.) The sites are also equipped with infrastructure facilities and required equipment such as personal computers, Participant Terminal System (PTS) access points, and so on. These out-of-region capabilities were certified as operational in mid-2003.

Redundant functionality -- The alternate sites are also equipped to sustain business functionality for periods of time. We have emergency power systems to ensure continuity in case of power outages. In addition, our most critical operating departments use at least two separate sites to process data, so that if one goes down, loses connectivity or becomes inaccessible, we can continue processing at the other. Moreover, to guard against the loss of data and ensure a flexible structure for quick recovery in an emergency, we now route communications from our customers among our widely distributed data processing centers on a daily basis.

Two-hour recovery – Tests conducted each year assure us that, in the event of a major disaster, DTCC can activate its out-of-region capabilities and resume data processing operations within the two-hour window stipulated in the interagency paper on business continuity issued by financial regulatory authorities in 2003. Depending on the circumstances around the loss of the New York data centers, DTCC might experience some loss of data on transactions processed immediately before its New York area centers are shut down when systems operations are recovered at the remote site. DTCC utilizes EMC's STAR replication technology for disk, so that in the event of a disaster in DTCC's northeast facilities, only data transmitted in the last minute prior to the time of the disaster should typically require retransmission at the disaster recovery center. Given the distances involved, however, it will not be possible to have synchronous data replication to the remote site for the foreseeable future.

Moving higher volumes of data over longer distances – Prior to the outfitting and testing of DTCC's remote data centers, accurate consistent data replication was seldom achievable much beyond distances of 30 miles. In conjunction with its technology partners, DTCC has implemented an innovative solution that takes data replication to a new level. The result is that we can now achieve high-speed asynchronous data replication over distances of a thousand miles and more. This functionality runs in the background, is fully transparent to users, requires no manual intervention and has no downside impact on the processing environment. The replication capacity, among other things, is what allows DTCC to function over a multi-level, widely dispersed disaster recovery infrastructure, and we will be further strengthening this capability every year. We believe our experience and the technology solution we have implemented may provide a useful model for other organizations in financial services to consider, and DTCC's technology staff is prepared to share this knowledge with interested participants.

Assembling high-end, highly responsive data storage systems – Concomitant with DTCC's ability to move huge volumes of data rapidly was the need for storage infrastructure that can accept and process the data quickly. DTCC was able, within a year to implement the high-end data storage solution including the storage management software needed to run it. In the course of this, DTCC automated many of the key functions including the ability to restart the highly complex replication process automatically after an interruption. DTCC puts these systems through exhaustive testing and routinely upgrades them to ensure non-disruptive operations.

Sustain a resilient communications network and telecom system

DTCC has increased the resiliency of its communications network and enhanced connectivity with all major customers to ensure that all its data processing locations can be linked not only to customers' primary business locations but also to their backup locations. DTCC is also mandating connectivity testing for these same customers at least once a year.

The SMART backbone – The backbone of DTCC's ability to communicate with customers is its network infrastructure, called the "SMART" (Securely Managed and Reliable Technology) network. The redundant telecommunications security engineered into the SMART network in the 1990s proved invaluable in the aftermath of September 11th, preserving DTCC's ability to interact with the major depository participants and continue depository operations throughout that week. Since 9/11, DTCC has moved aggressively to complete the task of building SMART into a seamless, end-to-end, managed communications system encompassing a geographically dispersed complex of processing centers, communications networks and control facilities. Each element of SMART is highly secure, engineered with multiple independent levels of redundancy, and capable of handling DTCC's entire clearance and settlement workload. SMART is resilient and, in effect, "self-healing," providing, for example, a web of multiple networks and back-up levels to deliver mission-critical data.

The SMART role in business continuity – All of DTCC's data processing operations, as well as the entire SMART complex, are fully redundant and can be controlled from any of DTCC's multiple command centers. SMART is a key element of DTCC's business continuity strategy. All components of SMART across the multiple centers are managed and used daily providing multiple levels of redundancy. Rather than maintain business continuity capabilities in standby, we treat all sites, networks and management centers as a unified complex that is always accessible. Customer connectivity to our processing complex is supported by several layers of

fallback capabilities, with each processing site able to communicate synchronously with peer sites over multiple connections. All these sites, in turn, are linked to all our customer firms through their SMART connections. As long as we can get an instruction to any of our multiple processing sites, SMART will route it to the site or sites responsible for processing it. This provides DTCC the flexibility to use any of its various redundant backup components at any of the multiple facilities at any time.

Protecting Telecommunications – DTCC provisions and manages all elements of its SMART complex—from DTCC's processing sites all the way though to its customers' premises, including communications hardware, software and the relationships with multiple telecommunication providers. Since we provision all elements of the network, we are able to register all communications circuits with the Department of Homeland Security's Telecommunications Service Priority (TSP) program for priority restoration in the event of an outage. The TSP program provides national security and emergency preparedness users priority restoration of telecommunications services that are vital to coordinating and responding to crises.

Remote command and control – With the creation of out-of-region capabilities, DTCC has also established a command center network that interconnects all DTCC's data processing capabilities while providing remote command and control of these capabilities from any of DTCC's other data centers. Customers' transactions and calls are now routinely routed among these different communications centers on a daily basis. This distributed "command and control" configuration provides an added level of recovery capabilities in the event a data center has to be evacuated even though its systems remain fully functional (and, in fact, these capabilities were exercised during the August, 2003 blackout in the Northeast United States). The command and control function is now actively rotated among the data centers on a regular basis, assuring that all data center staff have the necessary experience to run the production environment.

3. Managing Through a Crisis

Strengthen DTCC's continuity and control process

Since the experience of the business disruptions following the September 11 terrorist attacks, DTCC has extensively reconfigured its preparations for managing in a crisis, including the revision of its crisis management planning. DTCC had long-standing requirements that all business operations and support departments develop business contingency plans in which, among other things, the departments identify critical tasks to be performed during emergencies, list the recovery time objectives for each, and designate the staff responsible for performing those critical tasks. As part of more rigorous planning criteria, DTCC revised its crisis management control structure, which now consists of (1) an executive command team, (2) several subordinate command teams focusing on particular business areas, and (3) a crisis command center.

Executive command team – In the event of a crisis, the company would activate an executive command team to manage the company's response. This team is composed of senior executives from each of the company's principal line and staff departments including legal, human resources, executive management, information technology, operations, relationship management,

security, and facilities. Each team member has specific responsibilities in a crisis, such as employee communication, external communication, technology continuity, business relationships, government liaison and so forth. In addition, each team member has several people identified as back-ups to ensure that a particular area of expertise is covered. All DTCC subsidiaries are represented on the executive command team. Our executive rotation program, combined with multiple backups for each of the team members, minimizes the probability that all members of the command team and their backups will ever be in the same location together.

First-response action teams – At each of DTCC's operating locations the company now has designated "first-response" action teams to deal with immediate crisis situations. The location teams have taken on greater importance in coping with crises as DTCC has dispersed its facilities more widely across North America. The responsibility of the location teams is to respond to a crisis as it affects their specific location, facilities and staff, reporting their activities to a designated member of the executive command team. This creates a clearly understood chain of command and reporting structure with appropriately designated responsibilities for dealing with crisis situations from the bottom to the top of the organization.

Business continuity command groups – DTCC also now maintains three business continuity groups. The technology infrastructure group focuses on crisis response and business continuity for all aspects of the corporate data processing infrastructure, including computer operations, facilities, telecommunications, systems support, distributed systems and so forth. The operations continuity group has responsibility for ensuring operational and processing continuity, and the product management group is charged with making sure specific DTCC products and services are functional and can be accessed or, if there are issues affecting a particular business line, managing those issues to mitigate their impact on customers. Membership on the continuity command groups includes senior managers from each of those areas, as well as their backups. These groups also report up to designated members of the executive command team.

Crisis Command Center – DTCC has designated specific areas both in its headquarters location and at other locations as Crisis Command Centers for use by the executive command team. These centers are equipped with all the necessary data processing and telecommunications capabilities – including voice communications independent of DTCC's normal telecommunications system – to permit the team to quickly assemble, assess the situation, give appropriate direction to the operating units of the company in a crisis, and communicate with others outside DTCC even if DTCC's own voice communications systems are down. All DTCC operating areas also have public address system capabilities permitting senior managers to communicate directly to employees in the event of an emergency.

4. Keeping Customers and Regulators Informed

Instill confidence during a crisis by providing customers, markets and regulatory authorities the information necessary to assess the situation and make decisions

DTCC continues to work closely with government and industry groups to assess and mitigate potential risks to DTCC's own operations or operational recovery capabilities, as well as to the industry processes they support. DTCC participates in a program with New York City officials

to coordinate access to our various facilities during an emergency. We work with a range of industry organizations. And we continue to work with the various government agencies and units charged with overseeing the functioning and infrastructure of the financial services industry.

Crisis communication – One of our principal concerns is the capability to communicate broad, often non-technical information to our customers, the marketplaces and regulatory agencies during an emergency. Communicating during a crisis is paramount. In the meantime, the initiatives we now have under way are discussed below.

5. Testing business continuity plans

Conduct rigorous, regular testing of DTCC's continuity plans and contingencies

DTCC testing - For more than a decade, DTCC has routinely conducted regular emergency response tests and then evaluated the results. Since 9/11, however, DTCC has stepped up the scale and urgency of its formal contingency exercises and has begun conducting "tabletop" exercises more frequently throughout the year to test crisis management team knowledge and resourcefulness in the face of catastrophic events. DTCC conducts regular "tabletop" exercises to validate how its command teams would respond in the event of a catastrophic loss of the company's headquarters or other locations. As with real events, these various exercises involve debriefing sessions and checklists that are used to identify weaknesses or opportunities for improvement.

New testing methodologies also encompassed in the program include work transfer testing and unannounced testing.

Work transfer testing occurs when a business process is located in at least two separate facilities and the process can be completed in either facility. For testing purposes, one facility carries the daily work load while the other facility "stands down" and handles work other than the daily work load, e.g., aged items, etc.

Unannounced testing consists of activating the call tree portion of the BCP Plan. Senior Management activates the call tree outside normal business hours and notifies their respective business units of a hypothetical disaster situation. Employees are then instructed to report to work at their alternate worksite the following day to conduct business. For this type of testing, prior notification is not given to the employees to maintain the integrity of the test.

Work with customers to strengthen their business continuity plans and infrastructures

DTCC continues to work with its customers and other industry infrastructure organizations to discuss the industry's business continuity preparations and DTCC's expectations regarding customers' own business continuity capabilities. The *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* draws industry attention to a number of the

aspects presented by customer continuity planning, and some of the key steps we have taken to strengthen the industry in this regard are discussed below.

Ensuring connectivity – We have enhanced DTCC's telecommunications network with major participants to ensure continued connectivity from all our data processing locations not only to our customers' primary locations but also to their backup locations DTCC has met with several of its larger participants to review geographic diversity of their telecommunications and duplications and will continue to meet with others.

Connectivity testing –Each year, DTC, NSCC and FICC release Important Notices that establish telecommunications connectivity requirements for major participants and customers. We now require our larger-volume customers to test their connectivity with us at least once a year. This includes testing of connectivity from customers' primary and backup locations to several of the DTCC data processing locations.

Industry testing – In addition, DTCC participates in industry-wide testing with SIFMA and the FSA, as well as tests conducted by SWIFT and Fedwire.

Customer recovery planning – DTCC representatives participate in several industry committees focusing on business continuity issues at the industry level.

6. Business Continuity

As this paper has described, the experience of the disruptions following the terrorist attacks of September 11th led to a dramatic transformation in the thinking of DTCC and the industry about business continuity as an issue. Driven by that transformation, DTCC over the past several years has achieved a quantum leap in the level of resiliency in its systems and operations and in its preparedness to deal with crisis situations. Many industry members have implemented similarly sweeping changes in their business continuity practices.

In parallel with all of these efforts, our perspective has evolved to recognize the need for an even more sophisticated understanding and approach to aspects of the business continuity issue. The industry's overwhelming dependence on its information technology and telecommunications – the "fourth dimension" of cyberspace – creates new vulnerabilities that are thus far only partially understood. The complex web of interdependencies within the industry – both in its processes and its interactions – creates risks and "points of failure" that weaken our resiliency. The transformed nature of the threats we face requires a heightened level of coordination between the public and private sectors. And the increasingly international nature of the financial services markets demand greater coordination of business continuity practices across borders. The "next generation" of business continuity practices must be shaped by these new perceptions.

Coordinating between public and private sectors

The experience of September 11th also made clear that protecting the industry's critical infrastructure will involve significant levels of coordination between public sector and private sector organizations. The U.S. Department of Homeland Security is charged with this overall

responsibility in the United States, but DHS explicitly recognizes that the overwhelming portion of the nation's critical infrastructure is privately owned and, therefore, that infrastructure protection must involve the private sector to a major degree.

The U.S. Department of the Treasury has been named the lead agency with responsibility for infrastructure protection efforts for the financial services sector in the United States. The Treasury Department is assisted in this effort by the Financial and Banking Information Infrastructure Committee (FBIIC), a working group of representatives of the federal financial regulatory bodies.

Along with other financial industry organizations, DTCC is an active participant in the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), a private sector group that interfaces with Treasury and the FBIIC on infrastructure protection issues. The FSSCC works to coordinate the financial services industry's initiatives to protect critical financial services infrastructure. The goal is to ensure that these efforts focus on complementary objectives and contribute to achieving the highest possible level of overall industry resiliency. More information about the council may be obtained from its Web site: www.fsscc.org.

---

[i] *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System,* issued by the Board of Governors of the Federal Reserve System; Office of the Comptroller of the Currency; and Securities and Exchange Commission. April 7, 2003.

[ii] *Global Clearing and Settlement: a Plan of Action*, issued by the Group of Thirty. January, 23, 2003.