THE PAYMENTS RISK COMMITTEE

BEST PRACTICES TO ASSURE TELECOMMUNICATIONS CONTINUITY

FOR FINANCIAL INSTITUTIONS AND THE PAYMENT & SETTLEMENTS UTILITIES

Report by the Assuring Telecommunications Continuity Task Force

New York
September 2004

The Payments Risk Committee is a private sector group comprising senior managers from several major banks in the US, sponsored by the Federal Reserve Bank of New York. The Committee identifies and analyzes issues of mutual interest related to risk in payment and settlement systems. Where appropriate, it seeks to foster broader industry awareness and discussion, and to develop input on public and private sector initiatives. Current members of the Committee are Bank of America N.A., The Bank of New York, BankOne N.A., Citibank N.A., Deutsche Bank AG, HSBC Bank USA, J P Morgan-Chase, State Street Bank and Trust Company, and UBS AG.

1. EXECUTIVE SUMMARY

Financial markets are highly dependent on exceedingly complex telecommunications networks. The resiliency of these networks is crucial for the markets they serve and for the overall financial stability of our country.

There are practices that financial institutions and payment and settlement utilities that service them can adopt to avoid telecommunication outages and to facilitate rapid recovery when outages occur.

- In this report, we present thirteen Best Practices, outlined below.
- Throughout the report we also provide specific recommendations for measures that each organization can undertake in support of these Best Practices.
- The recommended Best Practices are widely applicable to all types and sizes of financial institutions and payment and settlement utilities.
- Best Practices should be adopted in a manner that is commensurate with each institution's size and risk profile. We believe that is neither necessary nor appropriate to prescribe any specific technology solution or to limit a firm's flexibility to implement the Best Practices.

BEST PRACTICES

#1: Establish policies and procedures covering vendor services, staffing, documentation, and security to facilitate sound telecommunications administration.

#2: Adopt Internet Protocol as the preferred telecommunications protocol.

#3: Configure communications links for maximum physical diversity.

#4: Regularly test backup facilities to ensure availability.

#5: Use SONET (or equivalent "self-healing" technology) to connect data centers to carrier central offices to make connections as resilient as possible.

#6: Consider the use of a variety of alternative technologies and services to address potential "last-mile" and inter-facility bottlenecks and single points of failure that cannot be resolved with conventional services.

#7: Concentrate multiple circuits to fewer, higher bandwidth circuits in order to simplify connectivity and better assure diversity.

#8: Adopt an "active-active" architecture where possible, with multiple mutually supporting active operational facilities and/or data centers.

#9: Consider multiple carrier networks for provisioning of circuits.

#10: Establish diversity criteria for carriers and develop audit programs to ensure compliance with the criteria.

#11: Conduct regular audits of telecommunications documentation and diversity.

#12: Design frame relay networks to avoid Network-to-Network Interconnects (NNIs) and reduce complexity and single points of failure inherent with some NNI connections.

#13: Assign responsibility for circuit monitoring and the initiation of troubleshooting and repair of circuits connecting financial institutions and a payment and settlement utility to the utility.

Readers of this Report should consult the Financial Services Task Force Report to the President's National Security Telecommunications Advisory Committee, which can be found on the National Communications System website, www.ncs.gov/nstac/nstac_publications.html.

Table of Contents

2. BACKGROUND

The Federal Reserve Bank of New York established the Payments Risk Committee in 1993 as a means of inviting the input of commercial bankers in formulating recommendations for improving the quality of risk management in payment and securities settlement systems. Senior executives with broad payments systems experience from banks active in the payments business were invited to participate in the Committee. In addition to its primary role of formulating risk reduction recommendations, the Committee's objectives are to promote better understanding of payments risk issues among market participants; enhance knowledge of the workings of particular payments systems in the U.S. and internationally and to circulate research on payment systems to participants and the public; promote better communication between private sector institutions and the Federal Reserve Bank and, where appropriate, other bank supervisors within the U.S. and internationally; and provide a forum for discussion of technical issues in payments systems.

The Committee is sponsored by the Federal Reserve Bank of New York and is composed of representatives of Bank of America N.A., The Bank of New York, BankOne N.A., Citibank N.A., Deutsche Bank AG, HSBC Bank USA, J P Morgan-Chase, State Street Bank and Trust Company, and UBS AG. There is also participation by the Federal Reserve Bank of New York and the staff of the Board of Governors of the Federal Reserve System. The Committee is supported by a Working Group of mid-level executives, which conducts research regarding topics designated by the Committee and drafts reports and studies for Committee approval.

2.1 The Working Group and Assuring Telecommunications Continuity Task Force

In 2003, the Committee requested that the Working Group create a paper describing steps that financial institutions can take, acting either individually or in concert, which could help to assure telecommunications continuity. The Working Group was directed to develop suggested telecommunications best practices for individual financial institutions and for the payment and settlement utilities serving the financial markets. Because there are a number of efforts already underway involving telecommunications resiliency that include the financial industry, the telecommunications industry, and government, the Committee asked the Working Group to also focus on those measures that financial institutions and the payment and settlement utilities can take at time of disaster, using only their own resources, without reliance on the telecommunications carriers or government.

Due to the broad scope of the topic "assuring telecommunications continuity," the Working Group assembled a Task Force to examine the issues and draft a report. The Working Group recognized the need to involve additional experts, and individuals representing payment and settlement utilities were recruited from outside of the Committee member banks. A full list of the members of the Task Force appears below.

2.2 Acknowledgements

Valuable guidance and support was provided by the members of the Payments Risk Committee and the Working Group. Additionally, considerable assistance was furnished by The Clearing House (TCH), The Depository Trust and Clearing Corporation (DTCC), the Securities Industry Automation Corporation (SIAC) and SWIFT.

The conclusions, recommendations, and best practices set forth in this Report do not necessarily represent policies of the institutions represented nor the policies or views of the Federal Reserve System.

MEMBERS OF THE TASK FORCE

Chairman	Mr. Ciro Vitiello, The Bank of New York
Co-Chairman	Mr. Carl Rosenberger, The Bank of New York
Team Leaders:	
Best Practices for Financial Institutions	Mr. Paul Miller, Deutsche Bank
Best Practices for Payment And Settlement Utilities	Mr. Albert Wood, The Clearing House
Cooperative Measures	Mr. Jeffrey Kuhn, The Bank of New York
The Bank of New York	Mr. Jeffrey Cohen Mr. Stephen Henne Mr. Jeffrey Kuhn Mr. Thomas Prusinski Mr. Carl Rosenberger Mr. Ciro Vitiello
Bank of Tokyo-Mitsubishi	Mr. Wesley Ward
Citibank	Mr. Kambiz Mofrad
Depository Trust and Clearing Corp.	Mr. William Aimetti Mr. Michael Obiedzinski Mr. George Perretti
Deutsche Bank	Mr. Oscar Menendez Mr. Paul Miller
The Federal Reserve Bank of New York	Mr. Gary Bertone Mr. Todd Waszkelewicz
J P Morgan Chase	Mr. James Le Mon Mr. Michael Ullman
State Street Bank and Trust	Mr. Joseph Lentini Mr. Joseph Lozito Ms. Kathleen Voigt
SWIFT	Mr. Neil Wilson
The Clearing House	Mr. Joseph Alexander Mr. Arthur Rosenberg Mr. Albert Wood
UBS AG	Mr. John McGarvey

3. TELECOMMUNICATIONS BEST PRACTICES

3.1 List of Best Practices

The following Best Practices are intended for financial institutions and payment and settlement utilities, but are generally applicable to any enterprise with telecommunications requirements. The list is not exhaustive, and a more focused implementation will naturally be required of larger institutions and utilities, both in their connections to each other, and in their internal connections linking data centers and major operational facilities. Naturally, there is significant overlap between those practices being recommended for financial institutions and those being recommended for payment and settlement utilities.

Several of the Best Practices listed below are also applicable to networks and circuits connecting financial institutions to their clients.

Each financial institution and payment and settlement utility should:

- Evaluate the risk of loss of connectivity to each client and, in the case of proprietary products and networks delivering payment and settlement services, to groups of clients.
- Seek to enforce Best Practices with impacted clients in situations in which a client or group of clients on the same network presents a risk of business disruption to either the institution or the financial markets in general.

Best Practice #1: Establish policies and procedures covering vendor services, staffing, documentation, and security to facilitate sound telecommunications administration.

Telecommunication responsibility should be centralized to the extent possible, and in a manner consistent with a company's organization and business mode, to provide consistent communications across all business lines and to ensure that redundancy and diversity objectives are met, that state-of-the-art techniques are being employed, and that consistent policies are in place, enterprise-wide.

Financial institutions and payment and settlement utilities should:

Vendor Services

- *Ensure that all vendors provide duplicated, non-co-located network elements, wherever possible, along with maintenance, administration, surveillance, and support for all components.*
- *Ensure all vendors comply with the prescribed service level agreements, recovery time objectives, and commitments to routing diversity.*
- *Utilize Direct Inward Dialing (DID), with a redirect option where available.* This option should provide fail-over options for all critical DID calls, and include a seamless fail-over option for outbound local and long distance calls.

Staff Planning

- *Maintain Network Operating Centers that are adequately staffed and geographically diverse, with UPS and generator backup power, as well as HVAC systems.*
- *Train and equip Help Desks with the appropriate monitoring and diagnostic tools and full network documentation.*

- *Grant employees secure and redundant remote access to the company's systems,* permitting them to operate, trade, or sell from home in the event that voice and/or data services are lost in their normal place of business and their contingency site is for any reason unusable or unreachable. Remote access capacity must be adequate to deal with increased volumes in times of emergency, with priority access granted to those employees performing critical functions.
- *Issue GETS cards to key employees* for use in contingency situations.

Documentation

- *Maintain a centralized database listing telecommunications equipment, as well as vendor information,* such as origination of the links, last-mile communication path, link endpoints, and criticality of the supported business function. Maintain an off-site, regularly updated backup of this database for use in contingency situations.
- *Create a communications structure, including an escalation list for critical service providers,* for timely notification of affected parties in the event of disasters or emergencies.
- *Develop a Telecommunications Business Continuity Plan* to ensure service continuity and provide for the orderly restoration of critical services in the event of a major network catastrophe.
  - *Delineate and identify disaster recovery services.*
  - *Where possible, solicit carriers to provide guarantees that the delivery of service is diverse.*
  - *Maintain this Plan on site and off site.*
- *Keep a list of identified potential single points of telecommunications failure, as well as planned mitigants.*
- *Include telecommunications management in the company's incident management process.*

Security

- *Strictly limit physical and logical access to telecommunications facilities to those who are authorized.*
- *Create and enforce telecommunications change control policies and procedures.*

Best Practice #2: Adopt Internet Protocol as the preferred telecommunications protocol.

Internet Protocol (IP) is an efficient, flexible, routable, and universally available communications protocol, and is widely used in a broad variety of applications. New applications involving communications, with rare exception, specify IP as the preferred method of communications. Older applications are being rapidly converted to IP in recognition of its superior qualities.

IP is rapidly gaining universal acceptance as the preferred communications protocol. As such, manufacturers and companies have invested, and continue to invest, considerable amounts of time and money into improvements for IP-based networking equipment and related

technology. Related IP protocols to support resilience are becoming ubiquitous and ever more robust.

Because of their inherent flexibility, IP connections can more easily share common communications facilities and realize economies of scale in applications where numerous connections exist. IP is ideally suited to support resilience and diversity needs, because re-routing and traffic load balancing are much easier to configure and support.

Financial institutions and payment and settlement utilities should:

- *Design all new applications to support IP.*
- *Modify older applications to support IP*, in addition to older legacy protocols. If legacy applications cannot be reasonably modified to support native IP, encapsulation of the protocol may be an acceptable alternative.
- *Use best efforts to implement information security best practices as part of the IP solution.* Since the topic of cyber-security is ever changing and evolving, financial institutions, their customers, and payment and settlement utilities must constantly monitor changes in best practices in this area and be prepared to continually improve IP security.

Best Practice #3: Configure communications links for maximum physical diversity.

Physical diversity (i.e., multiple, separate pathways or facilities with no common points of failure) is a critical line of defense against outages. However, to truly be effective, such diversity must be achieved at the shelf, switch, central office, manhole, and entrance to the building, multiplexor, and riser level.

In the provisioning of telecommunications services, financial institutions and payment and settlement utilities should:

- *Select services that are resilient, with redundant and physically diverse cable entrances to each building as well as diverse physical paths to independent central offices.*
- *Locate cable points of entry and separate cable vaults as distant from each other as possible.*
- *Design building risers so that they come up to appropriate floors in separate shaft ways and, if possible, terminate on different floors in the facility.*
- *Locate terminating equipment with as much separation as possible.*
- *Utilize separate and isolated power supplies, where possible, for terminating electronic equipment, with generator and/or UPS backup.*
- *Classify network elements (e.g., domain servers, signaling servers) essential for network connectivity as critical systems*, and manage them in a highly secure and resilient environment.
- *Assign Telecommunications Service Priority (TSP) status to critical circuits.*

Best Practice #4: Regularly test backup facilities to ensure availability.

Most circuits internal to financial institutions, and between financial institutions, their clients, and payment and settlement utilities, have some form of backup to safeguard against primary circuit failure. Backup arrangements can range from simple dial-backup connections to alternate leased lines at alternate data centers. If these connections are not tested on a regular basis, the connections may actually not be available or work when needed during a primary circuit failure.

Financial institutions and payment and settlement utilities should:

- *Perform quarterly testing of backup arrangements, at a minimum, if you are considered a "significant" institution,* as defined by the Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.
- *Exercise alternative pathways regularly, in production,* to ensure that they remain viable and capable of carrying a production workload.
- *Conduct "end-to-end" communications tests that include all external partners*: clients, payment and settlement utilities, and telecommunications service providers.

Best Practice #5: Use SONET (or equivalent "self-healing" technology) to connect data centers to carrier central offices to make connections as resilient as possible. When available, dedicated SONET is preferred to shared rings.

SONET (Synchronous Optical NETwork) technology provides highly resilient, high-capacity services that are used by carriers in their inter-office backbone networks.

SONET communicates through fiber-optic rings over two diversely routed paths that resemble a ring. If one path of the ring is disrupted, the electronics connected to the ring will automatically reverse the communication path and take the alternate route to reach any point on the ring. Switching takes place in milliseconds and is transparent to most communications applications.

Carriers will install SONET rings to connect their high-capacity customers to terminating Central Offices (COs). These rings can provide the same levels of resiliency that carriers achieve for their own networks. Rings can be dedicated with connections on the ring for data centers only and the carrier central office(s).

When establishing SONET service, financial institutions and payment and settlement utilities should:

- *Consider sharing the high-capacity rings with other subscribers needing similar connectivity, which can reduce expense.* However, dedicated rings are preferable, for security and reliability reasons.
- *Ensure street routing is on a ring configuration connected to multiple Points of Presence (POPs) or COs.*
- *Very carefully examine the physical routing of your SONET rings.*
  - *When possible, avoid routing rings through multiple buildings.*
  - *Avoid "collapsed" rings,* which occur when there are spots along the ring where both paths must physically traverse some common structure, such as a bridge over a river, or a tunnel. These common structures represent physical, single points of

failure that can "collapse" the ring and defeat the counter-rotating tactics for ensuring connectivity.

- ❖ When either of the above conditions is unavoidable, develop strategies for rapid recovery during a collapse.

Best Practice #6: Consider the use of a variety of alternative technologies and services to address potential "last-mile" and inter-facility bottlenecks and single points of failure that cannot be resolved with conventional services.

In cases in which a data center's geographic location makes it difficult to achieve diversity of traditional terrestrial telecommunications lines – as with remote data centers many miles from carrier end-offices and critical, high-capacity trans-oceanic circuits between data centers – financial institutions and payment and settlement utilities should:

- ➢ *Consider the use of a variety of alternative technologies and services to achieve appropriate diversity.* Some examples of alternative technologies include:
  - ❖ Wireless services such as satellite, microwave, and laser, which serve as an alternative path for high-bandwidth communications between data centers, and last-mile connections to carriers. These wireless technologies can be installed independently of existing terrestrial communications lines and therefore can provide a good solution for route diversity.
  - ❖ Non-traditional carriers or services such as cable television (CATV), electric utilities, and the Internet. These carriers typically use rights-of-way that are completely separate from traditional wire-line carriers and, because of their relatively recent entry into the market, often have modern equipment.

As these alternative technologies generally have limitations (e.g., insufficient bandwidth or latency) and are more costly, we recommend their use only for the most critical circuits and as an addition to, not as a replacement for, more traditional technologies.

Best Practice #7: Concentrate multiple circuits to fewer, higher bandwidth circuits in order to simplify connectivity and better assure diversity.

Payment and settlement utilities and financial institutions should work to consolidate large numbers of circuits between the same two physical facilities to a limited number of higher capacity, highly diverse circuits that will accommodate each company's application needs. Care should be taken during the consolidation process to ensure that circuit diversity is maintained.

Consolidation can make managing diversity a simpler task with a higher probability of success. When combined with the best practice of implementing TCP/IP for all connections, fail-over capabilities are greatly improved in both ease of recovery and recovery time. As an additional benefit, fewer, higher speed circuits may be less expensive than the sum of all the lower speed circuits.

Best Practice #8: Adopt an "active-active" architecture where possible.

An "active-active" architecture, featuring multiple active operational facilities and/or data centers that are mutually supporting, is the most resilient design, as transactions from a non-operational or temporarily disconnected site can be switched to the surviving facilities for processing. In such cases, all circuits are constantly tested by virtue of their regular use in production.

Financial institutions and payment and settlement utilities should:

- *Divide and route traffic between utilities and financial institutions across all data centers* in order to assure continuous operation of connections to all data centers.
- *Bear in mind that the most resilient connections between a financial institution and a utility are those that connect to geographically separated data centers and never converge.*
- *Continually split traffic among the connections and re-route as needed* to ensure these diverse connections are always working.
- *Conduct regular fail-over testing* to ensure that the fail-over scheme works reliably and that surviving circuits have adequate capacity to handle the extra traffic.

Best Practice #9: Consider multiple carrier networks for provisioning of circuits.

While use of multiple carriers is no guarantee of diversity, in some applications, it can result in fewer single points of failure in the combined network, especially if a financial institution's circuits are distributed across multiple carriers. In addition, use of more than one carrier can provide better logical diversity for the intelligent switching components in their networks.

Another approach to multiple carriers is the mixing of traditional and non-traditional carriers. Examples of non-traditional carriers would be power utilities and cable television providers that may have completely separate and diverse rights-of-way and switching facilities from those of traditional telecom carriers.

Financial institutions and payment and settlement utilities should:

- *When using multiple carriers, ensure the critical ability to obtain and correlate physical routes between the carriers.*
- *When ordering the circuits, take care to ensure that the multiple carriers are not sharing rights-of-way or other common transport elements in the paths.*
- When selecting alternate carriers, opt for facilities-based carriers – those that own their own cable routes, central offices, and related switching equipment. Some smaller carriers, especially in the local markets, are simply reselling the service of larger carriers. While appearing diverse, these carriers may be supplying service over the same facilities as another carrier being used to obtain diversity, thus creating a false impression of circuit diversity where none exists.
- *Thoroughly research each non-traditional carrier* to determine the true extent of its service area, interactions with traditional carriers, and its capacity and ability to serve the needs of demanding customers in a critical industry.

Each utility and financial institution should evaluate whether a multi-carrier or single-carrier strategy will provide it with better diversity and resiliency. In some cases, a "primary" vendor can do a better job of coordinating a variety of suppliers, because of the primary carrier's relationships with other carriers. In some cases, due to competitive issues, such relationships may not work, and the company may have the market leverage to get the needed routing information. Each situation is unique, and the approach therefore must be carefully crafted.

Best Practice # 10: Establish diversity criteria for carriers and develop audit programs to ensure compliance with the criteria.

Financial institutions and payment and settlement utilities should:

- *Work to establish criteria and best practices for validating carrier diversity.* Routing of services and identifying possible single points of failure are part of those criteria. These vetting processes should be published as a single document.

Best Practice #11: Conduct regular audits of telecommunications documentation and diversity.

Financial institutions and payment and settlement utilities should:

- *Perform periodic internal audits of telecommunications documentation,* including Service Level Agreements.
- *Perform diversification validation – to the extent practical given the limitations of carriers – at least twice annually* if the firm is classified as a "significant" or "core clearing and settlement" firm. At least one of these validations should include a physical validation of equipment compared to the recorded documentation of diversity.

Best Practice #12: Design frame relay networks to avoid Network-to-Network Interconnects (NNIs) and reduce complexity and single points of failure inherent with some NNI connections.

NNIs are logical and physical boundaries of frame relay networks that delineate the network of one frame relay provider from that of another. NNI connections are sometimes required in order to complete a frame relay connection from a utility to a financial institution. This can occur, for example, when a utility's frame relay provider's own network does not extend to the financial institution's location. In these cases, the utility can elect to interconnect the preferred frame relay provider to another frame relay provider that operates in the financial institution's service area through an NNI connection, or it can elect to install a standard private line from the preferred frame relay provider's nearest point of presence out to the financial institution.

NNI connections add complexity to a frame relay circuit and possible single points of failure because the information exchange between carriers on how these circuits are provisioned or routed can be complicated or poorly documented.

This complexity may result in delays in provisioning, delays in restoration, and confusion over the actual physical routing of circuits between a financial institution and a utility, or between a financial institution and its clients.

NNI connections are also concentration points where many circuits between two different frame relay providers are interconnected in mass quantities.

Financial institutions and payment and settlement utilities should:

- *Take care to diversify interconnects among the physical switching devices that provide the interconnection*; otherwise, all circuits between the bank and the utility could be located in a single switch, thus creating a potential single point of failure.
- *Avoid this situation by provisioning frame relay circuits that do not require NNI interconnects.* This can be accomplished by selecting frame relay providers with a network presence in the desired termination area, or by extending the preferred provider's network connection with a private line from the provider's nearest point of presence.

Best Practice #13: Assign responsibility for circuit monitoring and the initiation of troubleshooting and repair of circuits connecting financial institutions and a payment and settlement utility to the utility.

Mixed ownership of circuits connecting utilities and their financial institutions can create jurisdictional confusion, delay repairs, make the assignment of TSP status more difficult, and inadvertently create single points of failure.

Telephone companies will usually only discuss circuit issues with the customer of record of the circuit. Financial institution "ownership" can therefore make it difficult for the utility to contact the carrier when an outage is detected on the bank's circuit. The necessary involvement of the financial institution's technical staff, even to report the outage to the carrier, can introduce delay into the restoration process. Additionally, circuit ownership gives the utility the ability to monitor the circuit, end-to-end, for quicker identification of potential problems.

Coordination for diversity purposes can also be an issue. While a financial institution will understand and be able to correctly specify routing for a circuit into its own facility, it may not know much about routing into the utility facilities or about other network features that may be employed by the utility to enhance resilience. This lack of knowledge can lead to delays in provisioning and unintentional single points of failure. It may also be more efficient for a utility to obtain TSP certification for circuits compared with the processes that its individual financial institution clients may have.

Financial institutions and payment and settlement utilities should:

- *Ensure that, wherever possible, utilities are the end-to-end customer of record for their circuits*, including the tail circuit at the financial institution, to ensure diversity and to be able to assign Telecommunications Service Priority (TSP) status to the circuit. Although utility ownership of circuits is the simplest model, financial institutions will sometimes want to be the customer of record for circuits installed between themselves and the utility. Their reasons include the need for monitoring, trouble-shooting and escalation, expense control, security and the desire to direct circuits into specific facilities for resiliency purposes. This can cause conflicts for

utilities that are also trying to achieve the same objectives for their network services. Should the financial institutions insist on circuit ownership, or should particular circumstances favor financial institution circuit ownership, utilities should reach agreement with their client financial institutions to permit the utilities to monitor the connections and to initiate troubleshooting and/or repair activity. (Similarly, the Committee recommends that a financial institution seek, where possible, to be the customer of record for its links to clients. The Committee recognizes, however, that clients may not be willing to concede circuit ownership to their financial institution in all cases.)

- *Employ a standardized ordering process.* A standard ordering process for institutions and utilities will alleviate much of the concern that a financial institution may have regarding ordering and routing of circuits. (See the Appendix to this Report for a sample standardized ordering process developed by the Task Force and endorsed by The Clearing House and the Depository Trust and Clearing Corporation.)
- *Assign TSP status to all critical circuits.* All parties must be sensitive to the fact that, during an emergency, TSP circuits provide significant recovery advantages over all other arrangements. In a crisis, telecommunications carriers must, by law, restore TSP circuits prior to all other circuits, even if the other circuits are covered by a service level agreement under which the carrier has promised a premier service.

4. ALTERNATIVE APPROACHES TO ASSURING CONTINUITY

4.1 Overview:

The Task Force focused on several new alternatives to existing networks and for new, more highly available, networks to be leveraged across the financial services industry. The industry utilities have been developing highly resilient networks that need to be utilized more broadly, even if only for contingency purposes.

The Task Force also reviewed different approaches for the participant banks to share their proprietary networks. Although this concept is technically feasible, it was decided that organizational and coordination issues render it impractical. The larger financial institutions are able to negotiate preferred service levels from the major telecommunications vendors and have dedicated staff to ensure that the service provided meets their needs. In addition, if they can be connected to multiple industry networks there is another level of redundancy that allows the participants to have multiple access points to the utilities.

4.2 Utility Network Solutions: Current Situation and Future Plans

4.2.1 Fedwire

Currently, the Federal Reserve does not have a fully IP-based network to connect participating financial institutions to Federal Reserve services. Since its move to frame relay, the Federal Reserve is encapsulating their SNA traffic within IP, and is working on plans to convert both the computer interface customers and the FedLine® customers to a fully IP-based network. This conversion will take place over the next several years with FedLine customers moving first, followed by the computer interface customers. The Federal Reserve plans to have a series of seminars with computer interface customers to describe its approach to this migration and to solicit input on the design of its solution and the timing of implementation.

The Federal Reserve is currently working on a pilot project that would provide the capability for customers to transport current formatted Fedwire® Funds Service messages to the Federal Reserve via SWIFTNet. This alternative communication path would provide a contingency option in scenarios where either the Federal Reserve's network (FEDNET®) is unavailable or an individual financial institution's FEDNET connections are unavailable. This project is being piloted with customers and application vendors during 2004. After the pilot project is complete, the Federal Reserve will evaluate with its customers, the interest/value of this service offering. Assuming that these are positive, the Federal Reserve would look to offer this alternative connection to all Fedwire Funds Service customers in 2005. The next step would then be investigating the use of this mechanism for Fedwire Securities Service messages.

4.2.2 CHIPS

The current CHIPS network is based on an X.25 protocol that is over ten years old and is nearing the end of its useful life. While the network is in no danger of failing, and The Clearing House (TCH) has taken steps to ensure that it can be maintained for the immediate future, TCH recognizes the need for a successor network for CHIPS and has put in place a procedure to replace the existing network with a TCP/IP network by the end of 2005. TCP/IP was chosen because of (i) the wide availability of products to implement TCP/IP; (ii) TCP/IP is widely implemented in most banks, as well as on SWIFT and, soon, on Fedwire; (iii) TCP/IP will provide the CHIPS network with increased flexibility and resilience for CHIPS connections; and (iv) the increased speed that TCP/IP affords.

The Clearing House considered building its own TCP/IP network for CHIPS or entering into an arrangement with SWIFT to allow CHIPS participants to connect to CHIPS over SWIFTNet (see section on SWIFT, below). CHIPS participants were surveyed, and some banks were concerned about the concentration risk that could result if CHIPS were to use SWIFTNet.

Based on this feedback, TCH has determined to go forward with both options, offering CHIPS participants a choice of connecting to CHIPS over a new CHIPS network based on TCP/IP or connecting to CHIPS through SWIFTNet. This approach has the advantages of giving the banks a choice and giving the system needed redundancy. The new connections will be available for CHIPS participants by the end of 2005.

4.2.3 SWIFT

SWIFTNet is an IP-based messaging infrastructure for SWIFT's messaging services that are provided over SWIFT's Secure IP Network (SIPN). Customers connect to the SIPN backbone over access networks provided by SWIFT's network partners.

The SWIFTNet messaging services offer secure, interactive (real-time) messaging, file transfer and browsing capabilities using SWIFT's mandatory software, SWIFTNet Link, and SWIFTNet Public Key Infrastructure (PKI) for security. This provides IP connectivity instead of X.25 connectivity.

A recent release of SWIFTNet provided for a new service called File Act. File Act can be used to exchange files generically between financial institutions, on a bilateral basis. File Act is a new application and will need to be analyzed further to determine how it could be used in a contingency situation.

4.2.4 Depository Trust and Clearing Corporation (DTCC)

The DTCC operates multiple data centers that are fully redundant, geographically dispersed, and fully staffed. In addition, there are multiple active network hubs with traffic automatically routed to production destinations without any DTCC participant intervention. The IP-based network that connects participants to DTCC is called SMART (Securely Managed and Reliable Technology). SMART is based on frame relay and has multiple carriers for diversity. All traffic is routed from the participants to all DTCC data centers. SMART is owned and managed by DTCC, end-to-end. All circuits are registered with the Federal Government under the TSP program.

4.2.5 Securities Industry Automation Corporation (SIAC)

The SIAC IP-based network is called the Secure Financial Transaction Infrastructure (SFTI). This network eliminates last mile vulnerability in connections from industry participants to SIAC data centers and from SIAC data centers to the NYSE and AMEX. SIAC guarantees network diversity through four access points in the New York Metro area (midtown and downtown Manhattan, New Jersey and north of NYC in Westchester), as well as two additional access points in the Midwest and New England. The SFTI network is comprised of redundant SONET rings and several different carriers. SIAC is also researching access points in other locations in the U.S., London, and in continental Europe. All participants are required to have multiple diverse access points into the SFTI network.

4.3 Alternative Approaches:

Analysis of developments in the industry suggests two non-exclusive approaches to diversity that can be pursued simultaneously - SWIFTNet as an alternate on the payment side for CHIPS and Fedwire (for funds), and mutual backup for the securities utilities through a combination of SFTI and SMART.

4.3.1 Payment Transactions

As discussed above, the Federal Reserve has begun a pilot project with SWIFT to leverage SWIFTNet as an alternative to the Fedwire Funds Service for sending and receiving fund transfer messages. (Depending upon the success of this effort, the Federal Reserve may elect to extend this program to the Fedwire Securities Service.) Similarly, CHIPS is also working with SWIFT to allow large value payment transactions to be passed via SWIFTNet in addition to accepting them over its own TCP/IP Network. SWIFTNet is content independent but does require that the messages be encapsulated. This alternative solution addresses potential problems where FEDNET, CHIPS, or a region of the U.S. telecommunications network is not functioning.

The Payment Risk Committee encourages all financial institutions using either the Federal Reserve's Funds Wire or The Clearing House CHIPS network to pursue alternate connectivity through SWIFTNet.

4.3.2 Securities Transactions

It appears that an alternative is already available in the area of securities transactions. DTCC's SMART network is already connected to four geographically dispersed SFTI Access Centers. Traffic can move either from SMART to SIAC or from SFTI to DTCC. SMART users can access SIAC-hosted applications and SFTI users can access DTCC-hosted clearing corporation applications. There do not appear to be any technical limitations for clients of either network to use these networks as alternatives to accessing DTCC and SIAC.

The Payment Risk Committee encourages all qualifying financial institutions with securities traffic to join both SFTI and SMART, in order to avail themselves of the diversity that the SFTI-SMART interconnection provides.

4.4 Issues and Challenges:

Many issues and challenges must be understood before these alternative solutions can be more broadly implemented. Policy conflicts in the area of security may exist. Consistent password and encryption techniques and/or the use of hardware devices must be agreed upon. The Federal Reserve's protocol of LU0 over SNA is extremely efficient and fast, and service level agreements may be impacted when high volumes are sent over SWIFTNet. Customer support and the responsibility for resolving problems can be complex. Testing and recovery are also areas in which extensive discussion would be required and agreement would need to be reached.

5. NEXT STEPS

5.1 Develop a Common Ordering Process For Telecommunications Links.

Many of the largest users of clearing and settlement utilities own dedicated, diverse physical connections from their data centers to multiple carriers and diverse central offices. Even smaller financial institutions may have preferences for the physical routing of a connection into their data center.

One problem faced by utilities is that often a contact at a financial institution is in the business operations area of the financial institution, and does not have knowledge of the preferred routing for utility circuits. Information on how to route circuits into the bank's data center is sometimes not readily available, especially if the utility is not working directly with the financial institution's telecommunications area. This results in circuits whose installations are delayed, that are incorrectly installed, or are non-optimally or improperly routed into the financial institution's facility. If situation remains undetected by the utility and the financial institution, false assumptions regarding diversity can be made, leaving the financial institution exposed to potential single points of failure in its connections to its utilities.

The responsibility for obtaining proper routing information is shared by both the utility and the financial institution. Utilities must continually educate their clients on the benefits and need for circuit diversity. Financial institutions must work to ensure a good and ongoing "connection" between their telecommunications departments and the utility so that correct routing information can be obtained.

Utilities and financial institutions on the Task Force are attempting to jointly develop an installation process that will address the needs of utilities to get the routing information they need to order circuits for their client financial institutions. If this effort is successful, all utilities should adopt this ordering process and conduct an outreach program with all of their clients to educate them regarding the process.

5.2 Follow-Through On Approaches To Diversity.

Although many issues – legal and technical – need to be reviewed, The Payments Risk Committee believes there is a great degree of potential to leverage the networks – SFTI, SMART, and SWIFTNet – that are either in place or emerging today. The PRC believes that the next step should be to convene two teams:

- Managers from payment and settlement utilities should meet to address high-level issues, such as system governance and liability boundaries, relating to utility inter-connectivity.
- A team of telecommunications technical experts from the payment and settlement utilities and financial institutions that they serve should meet to address the issues and challenges discussed above, and to create working and robust alternative pathways into DTCC, SIAC, CHIPS, and Fedwire.

To be filled out by Application Service Utility
Service Utility Name: Chose one
Participant Name:
Other required forms to accompany this form:
Change Control Number/Tracking Number/Ticket Number:

Type of service provisioned	**POTS**	**ISDN**	**DSO**	**FRAC T1**	**T1**	**DS3**	**Other**
Primary Site	☐	☐	☐	☐	☐	☐	
Contingency Site	☐	☐	☐	☐	☐	☐	

Contact information of the person completing this form

Name:
Title:
Telephone:
Email:
Please check if additional supporting documentation or diagrams accompany with form. ☐

Participant Primary Site Address	**Participant Secondary Site Address**
Address: City: State: Zip: Hours of access: Demark location: Floor: Room: NPA NXX: Participant Change Control Number/Tracking Number/Ticket Number:	Address: City: State: Zip: Hours of access: Demark location: Floor: Room: NPA NXX: Participant Change Control Number/Tracking Number/Ticket Number:

LOCAL ACCESS Identify owned or leased local access facilities for both sites. Letter of Agency needed to connect to Private Facilities.	
Service Provider: Secondary CFA to connect to: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:	Service Provider: Secondary CFA to connect to: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:
Service Provider: Secondary CFA to connect to: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:	Service Provider: Secondary CFA to connect to: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:
Service Provider: Secondary CFA to connect to: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:	Service Provider: Secondary CFA to connect to: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:

LOCAL ACCESS Identify Shared or Public facilities for both sites	
Service Provider: Identify LEC Mux IDs: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:	Service Provider: Identify LEC Mux IDs: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:
Service Provider: Identify LEC Mux IDs: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:	Service Provider: Identify LEC Mux IDs: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:
Service Provider: Identify LEC Mux IDs: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:	Service Provider: Identify LEC Mux IDs: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:

LOCAL ACCESS Copper Facilities	
Service Provider: Identify Cable IDs: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:	Service Provider: Identify Cable IDs: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:
Service Provider: Identify Cable IDs: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:	Service Provider: Identify Cable IDs: NPA NXX of LEC Servicing Wire Center: Special route mapping instructions:

INHOUSE WIRING EXTENTION from the DEMARC to the CPE Chose one of the following

PRIMARY Installation Contact **Primary DTA Site**	**PRIMARY** Installation Contac**t Secondary DTA Site**
Name: Title: Telephone: Beeper/Cell: Fax: Email:	Name: Title: Telephone: Beeper/Cell: Fax: Email:
ALTERNATE Installation Contact **Primary DTA Site**	**ALTERNATE** Installation Contact **Secondary DTA Site**
Name: Title: Telephone: Beeper/Cell: Fax: Email:	Name: Title: Telephone: Beeper/Cell: Fax: Email:

Telecommunications Service Installation Questionnaire

This questionnaire is being provided to you because your institution has signed up for a service from _____. It was designed to assist Application Service Utilities (ASU) such as the Federal Reserve Bank, The Depository Trust and The Clearing House to identify existing telecommunications facilities located at Member Financial Institutions (MFI).

This questionnaire will assist the ASU in utilizing existing facilities (if possible) your institution may have installed to ensure the most appropriate and resilient telecommunications links/circuits are utilized.

When the business office of an ASU receives a request for service from a MFI the order transitions to the group responsible for procuring telecommunications services. This group will assess the need for service and identify which types of service are needed. The procurement group will check-off the types of services needed on the top block of the Installation Questionnaire and send it to the appropriate area with-in the MFI for completion.

Who should receive the attached questionnaire at the MFI? The Telecommunications, Network or Facilities group that is responsible for telecommunications services. This is the group with your institution which manages and/or orders telecommunications circuits. This group should have a clear understanding of the Telco Service Vendors and types of services installed in the proposed sites or buildings.

The types for services that are important to identify: All privately owned or leased SONET rings; shared or public SONET rings; fiber Muxes (multiplexers) and copper pair cables for POTS and basic rate ISDN.

Instructions for filling out the Installation Questionnaire

Contact information of the person completing this form

- Provide *Name, Title, Telephone number and E-mail* address of the person filling out this form.
- *Please check if additional supporting documentation or diagrams accompany with form.* ☐ Check this box if you are sending additional information not found on this form.

Participant Primary and Contingency Site Address

- Fill-in the *Street Address, City, State* and *Zip Code* where the circuit are to be installed.
- List the *Hours of Access* available to service providers to install circuits.
- Identify the *Demarc Location, Floor* and *Room.* Example: Building 7, third floor, telecom room.
- *NPA NXX* the area code and exchange at the site
- *Participant Change Control Number/Tracking Number/Ticket Number*. The tracking mechanism used by the participant to control the installation process.

LOCAL ACCESS Identify owned or leased local access facilities for both sites.

- *Service Provider:* Telecommunications Providers (Verizon, MCI, AT&T and SBC, etc.) *Secondary CFA to connect to:* Connection point where service provider will connect to a circuit on this Sonet ring.
- *NPA NXX of LEC Servicing Wire Center*: The Area Code and exchange of the Central Office connecting to the ring.

LOCAL ACCESS Identify Shared or Public facilities for both sites

- *Service Provider:* Telecommunications Providers (Verizon, MCI, AT&T and SBC, etc.)
- *Identify LEC IDs*: Identify the Mux that or Sonet identification numbers list on the equipment.
- *NPA NXX of LEC Servicing Wire Center:* The Area Code and exchange of the Central Office connecting to the ring.

LOCAL ACCESS Copper Facilities

- *Service Provider*: Telecommunications Providers (Verizon, MCI, AT&T and SBC, etc.) *Identify Cable Ids*: Identify cable numbers of installed copper service.
- *NPA NXX of LEC Servicing Wire Center*: The Area Code and exchange of the Central Office connecting to the ring.

IN-HOUSE WIRING EXTENTION

Choose either Telco-provided or end-user-provided.

Primary and Secondary Installation Contact for both sites

Provide *Name, Title, Telephone number, Beeper, Cell phone number, Fax number and E-mail* address of the persons responsible to coordinate the installation at the end user.