

Testimony of
John R. Mohr
Executive Vice President
The Clearing House Association L.L.C.
U. S. House of Representatives
Committee on Financial Services
September 8, 2004

My name is John Mohr and I am an Executive Vice President of The Clearing House which is headquartered in New York. It is the oldest and largest clearing house in the United States and is owned by 19 very large global, international and regional banks. Founded in 1853, The Clearing House is a private-sector, global payment systems infrastructure that clears and settles more than \$1.5 trillion per day. It also serves as an industry forum addressing strategic and regulatory issues dealing with payments made in U.S. dollars.

The Clearing House serves more than 1,600 U.S. financial institutions and manages payment services that span the entire spectrum of paper, paper-to-electronic, and electronic payments. Services include local and regional check exchange and settlement services; ACH association and operations; large-value "wire" payments; electronic check presentment; and check image exchange. Financial institutions of all sizes benefit from this unique blend of payment systems that meet the highest standards for reliability, security and service.

I want to thank you for this opportunity to update you about steps which we have taken

to further strengthen the key elements of the U.S. payments infrastructure which are operated by The Clearing House.

One of the key lessons learned from the 9/11 disasters was that from a business continuity perspective “business as usual” was no longer adequate. Contingency and business continuity plans needed to be re-evaluated and refocused.

A major part of the original mission of The Clearing House was to “...promote the interests of its members and to maintain conservative banking through wise and intelligent cooperation.” Safety and soundness of the payment system has always been, and continues to be, part of the mission of The Clearing House, and one of our highest priorities.

One of the key reasons our large value payment system, CHIPS, was developed was to address the risk of high-value paper payments. As electronic payments became increasingly important to banks and their customers, TCH focused on the resiliency of its electronic systems. Over the years, TCH has developed a long-standing reputation for producing and managing high-quality software and observing conservative operating practices. TCH was among the first in the industry to operate fully redundant backup sites equipped with uninterruptible power supply (UPS) systems and diesel generators. And the results of these efforts speak for themselves - CHIPS has operated at the highest levels of systems availability since the early 1980's with system availability at or above 99.9%.

Since Sept. 11, 2001, the financial industry has increased its focus on the resiliency of its high-value payments systems. It is universally agreed that systems such as Fedwire and CHIPS must be capable of resuming full capacity operations quickly, within hours of any catastrophe. This is because of the reliance that the financial market places on the high value payments systems for intra-day liquidity and final settlement of their transactions. Without high value payments to “grease the wheels”, most financial markets would quickly grind to a halt.

TCH takes this responsibility seriously. It is worth noting that CHIPS never skipped a beat on Sept. 11, and the days that followed. CHIPS itself operated without interruption during the entire crisis and all of the 56 banks that connect to it were able to continue to conduct business. This included the 19 banks that were located in or near the World Trade Center. Each of these banks was required to relocate their operations to their contingency sites in the middle of an unimaginable disaster. The fact that this was successfully accomplished is a great testament to the leadership in these banks.

Following Sept. 11, TCH management reviewed the events of that week for lessons learned. We then reviewed our operations with those lessons in mind looking for ways to improve on the way that we conduct our business. We added additional security staff to perform more frequent and random patrols of our facilities. In addition, a private firm was hired to try to break into our physical and electronic security systems. Based upon findings from those penetration tests, we reconfigured one of our facilities and

implemented state-of-the-art biometric access controls. We implemented an ongoing testing program in place that includes periodic attempts to penetrate our systems to ensure that we maintain high levels of security. We also all but eliminated visitor access to our operating centers.

We reviewed where our critical employees work and relocated some of these individuals to avoid concentration of our workforce and to ensure that the talent needed to maintain and manage our operations is available in the event that we lose one of our sites. We have taken measures to ensure that key operations and support staff have secure remote access to our electronic systems for remote support. In addition, these individuals have Government Emergency Telecommunications Service (GETS) cards which allow them priority access to the public switched network in times of crisis.

For many years, TCH has operated fully redundant data centers, with each capable of backing up the other. All transactions are instantaneously replicated in the backup data center over a private fiber optic ring that interconnects the sites. In addition, CHIPS has customized software that constantly monitors the communications switches of its telecommunications providers and allows for rapid, automatic switching to the backup site. A switch from the primary operations site to the backup site can be accomplished in less than 5 minutes.

To further enhance its resiliency, TCH has developed an out-of-region tertiary data center. This new center is fully equipped to take over operation of CHIPS within an hour

of a simultaneous failure of the other two CHIPS data centers. Using custom mirroring software that was specially developed by The Clearing House, CHIPS was able to conquer the distance limits of synchronous mirroring technology and achieve recovery times consistent with synchronous mirror sites.

Mandatory testing of contingency capabilities has been conducted by CHIPS since the early 1980's. Requirements for mandatory testing and participant backup systems are incorporated into the rules that govern the operation of CHIPS. All users of CHIPS must agree to these rules as a condition of participation in the system. Backup capabilities are tested with the CHIPS community on a quarterly basis. The tests cover a variety of disaster scenarios and exercise the backup and recovery capabilities of the participants, as well as CHIPS. The performance of each participant during these tests is evaluated by The Clearing House and those banks that fail the test are required to continue to retest until they pass. The discipline of regular testing helped contribute to the quick recovery of the banks following the events of 9/11.

Resiliency cannot be achieved in isolation. Global cooperation among all the high-value payment system participants is essential. TCH understands this and actively participates in a number of industry groups dedicated to promoting the resiliency of this critical financial infrastructure. TCH is a member of the SWIFT Resiliency Advisory Council (RAC). In addition, TCH is a member of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security – a public/private group that advises the US Treasury and Dept of Homeland Security on matters of critical

infrastructure protection. TCH also works closely with Fedwire to explore ways to further develop best practices for sound operations and cross-system backup and testing.

When it comes to the safety and soundness of the global payments system, The Clearing House never rests. Backed by its Owner Banks – many of whom are leading experts in the payments industry, TCH promotes the cause of conservative banking practices through the development of best practices, expert commentary on banking regulation and policy and impeccable operations.

Another significant initiative led by The Clearing House following the events of 9/11 was our “Intercept Forum” which addressed the question “What could financial institutions, working with the public sector, do to eliminate the flow of funds to terrorists and their organizations?” We had senior representatives from 34 public and private sector organizations (see attached list). This forum identified five task groups which were co-lead by representatives from both the public and private sectors. These groups and their missions were:

Patterns of Behavior, whose mission was to identify the patterns of behavior of terrorists’ funding so that proactive steps may be taken to diminish and ultimately eliminate the flow of funds to terrorists.

Control List, whose goal was to review and confirm that existing and new policies, processes and requirements for obtaining and gathering information about suspected

terrorists and reporting that information to the appropriate government agencies are in place and working appropriately.

Account and Transaction Monitoring was charged with developing procedures and policies to identify and monitor transactions and/or account opening activity related to terrorist activity.

Global Cooperation and Best Practices focused on issues beyond our borders. It was clear that making changes only in the U.S. would simply drive terrorist financing to other countries. Therefore this team worked globally to remove obstacles to the flow of information needed to counteract terrorist financing and to export “Best Practices” to cooperating countries.

The **Database** team had a mission to develop a highly secure, real-time capability for regulatory and law enforcement agencies to download suspected terrorists/terrorist organizations “identities” to financial institutions seeking account and/or transaction hits which in turn would be uploaded to the respective agencies.

The Intercept Forum is a great example of the private and public sectors’ ability to work together to achieve shared goals. Financial institutions, law enforcement agencies and regulators were able to draw upon each other’s core competencies in a cooperative way and achieve meaningful results. It is clear that going forward we will need continued cooperation in all three areas in order to be successful.

Attachment A

Clearing House Owners

The Clearing House is owned by the following banks or their U.S. commercial banking affiliates: ABN AMRO Bank, Bank of America, The Bank of New York, Bank of Tokyo-Mitsubishi/Union Bank of California, BB&T, Citibank, Citizens Bank, Comerica Bank, Deutsche Bank, HSBC Bank, JPMorgan Chase Bank, KeyBank, M&T Bank, National City Bank, PNC Bank, SunTrust Bank, U.S. Bank, Wachovia Bank, Wells Fargo Bank.

Attachment B

Intercept Forum

Participating Organizations

Financial Institutions

ABN AMRO
Bank of America, N.A.
The Bank of New York
Bank One, N.A.
Citibank, N.A.
Deutsche Bank
FleetBoston
HSBC Bank
J.P. Morgan Chase & Co
Wachovia
Wells Fargo
Goldman Sachs

Associations

American Bankers Association (ABA)
American Council of Life Insurers (ACLI)
American Insurance Association (AIA)
New York Clearing House (NYCH)
Securities Industry Association (SIA)

Government Agencies

Department of Justice
Federal Bureau of Investigation (FBI)

Federal Deposit Insurance Corporation (FDIC)
Federal Reserve System, Washington, D.C. (FRB DC)
Federal Reserve Bank of New York (FRBNY)
Financial Crimes Enforcement Network (FinCEN)
New York State Banking Department
Office of Comptroller of the Currency (OCC)
Office of Foreign Assets Control (OFAC)
Office of Thrift Supervision (OTS)
Secret Service
Securities and Exchange Commission (SEC)
U.S. Attorney's Office, Southern District, New York
U.S. Department of the Treasury

Other

Sullivan & Cromwell
Depository Trust & Clearing Corporation (DTCC)
FDC/Western Union