For Release on Delivery
9:30 a.m., EST
February 21, 1990

Testimony by

Wayne D. Angell

Member, Board of Governors of the Federal Reserve System

before the

Subcommittee on Telecommunications and Finance

of the

Committee on Energy and Commerce

United States House of Representatives

February 21, 1990

Mr. Chairman and members of the Subcommittee on Telecommunications and Finance, I am pleased to appear today to discuss with you issues related to the security of large-dollar value electronic funds transfer systems and the influence of technology on the future development of these systems. The security of funds transfer and financial message processing systems is the subject of the General Accounting Office's January 1990, report Electronic Funds Transfer: Oversight of Critical Banking Systems Should Be Strengthened.

My testimony is divided into three parts and addresses topics identified by the Subcommittee as being of particular interest. First, I will provide an update on progress with respect to implementation of the GAO's recommendations addressing security on Fedwire, the large-dollar funds transfer system operated by the Federal Reserve Banks. Second, I will provide the Board's views on the need for clarification of its authority to oversee other funds transfer and financial message systems, such as CHIPS and S.W.I.F.T. Finally, I will provide a broader perspective on future technology trends as they will influence the international financial marketplace, with particular reference to payments networks.

As background to the update on the Federal Reserve's response to the GAO recommendations regarding Fedwire, it may be useful to highlight three distinguishing features of this system. First, the modern technology base that serves as the automation "platform" for Fedwire has evolved from decades of experience in

applying new technology to meet business requirements. The electronic transfer of reserve balances on the books of the Federal Reserve Banks began in 1918, using the telegraph. Today, the Federal Reserve uses state-of-the-art computers and data communications to operate Fedwire and is investing in research and development to ensure that the most current technology is used effectively, with a strong focus on security. Second, Fedwire is truly the nation's funds transfer system. All depository institutions have access to Fedwire and the Reserve Banks currently connect over 11,000 endpoints in all parts of the nation. These endpoints include the smallest to the largest depository institutions. As a truly national payment system, Fedwire must be responsive to a variety of needs presented by depository institutions having diverse characteristics. Third, Fedwire is the chief vehicle for effecting immediate final settlement for U.S. dollar payments, that is, the irrevocable transfer of value on the books of the Federal Reserve Banks, regardless of whether the payment originated domestically, or in London or Tokyo and was sent through a U.S. banking office. In short, when describing the role of Fedwire for settling interbank dollar transactions, it is no exaggeration to say that "the buck stops here."

As noted in the Board's November 9, 1989, response to GAO's draft report on oversight of electronic funds transfer systems, the Federal Reserve is strongly committed to providing the most secure electronic payment services possible. Such a commitment is essential in the case of a funds transfer system like Fedwire that handles about 240,000 transfers each day with

an average value per transfer of $3.1 million. We believe that it is important to begin any discussion of Fedwire security, as did the GAO, with the statement that there have not been any reported incidents (I can say with assurance no incidents) of fraudulent transfers by the employees who operate the system. Moreover, in the case of Fedwire, the same holds true for so-called interloper fraud.

The Federal Reserve's commitment to security begins with a sound Fedwire security "architecture," or unified structure of security safeguards and features which, in combination, define an organization's approach to security. The Federal Reserve security architecture incorporates a wide range of safeguards, which total over 100. These safeguards are, by the way, the result of our work with an outside consultant. To put the GAO recommendations in the proper perspective, it is important to understand the Federal Reserve's overall security architecture. I would now like to take a few moments to describe the safeguards and mechanisms that protect the Fedwire system within the overall security architecture.

The Fedwire safeguards are grouped into the following categories:

-- Physical security - to limit access to terminals and computer operations areas to those individuals who require access to perform their duties. Guards, surveillance equipment, and card key access devices are relied upon to prevent and detect unauthorized physical access to restricted computer spaces.

-- Access controls - both software and code words, to prevent unauthorized access to sensitive data and programs.

-- Encryption - to protect the confidentiality and integrity of Fedwire transactions, especially from interlopers. Nearly 100 percent of transmissions between depository institutions and Reserve Banks are encrypted and, as I will discuss later, the "backbone" communications network that links the 12 Federal Reserve Banks will be encrypted by July 1990.

-- Administrative controls - to govern employment practices, separation of duties, and software development standards.

Capacity planning and disaster recovery programs are also key components of the architecture to ensure that Fedwire provides secure and reliable services. In recent years, Fedwire computer uptime has improved steadily as a result of added attention to the need for a secure, resilient, and reliable automation environment. For example, in 1987 and 1988, Fedwire computer uptime averaged 99.14 and 99.21 percent, respectively. In 1989, Fedwire computer uptime averaged over 99.71 percent. I might note that last year's uptime statistic covers the period of the October 17, 1989, San Francisco earthquake. As a result of careful preparation and skillful action on the scene, the Federal Reserve Bank of San Francisco was able to recover operations quickly after the earthquake with no disruption to electronic payments processing.

We welcome the opportunity to refine the implementation of the security safeguards that make up the Fedwire security architecture by responding to the recommendations recently made by the GAO. The GAO's recommendations represent opportunities to tighten further the implementation of a very solid security architecture.

We agree fully with 15 of the 17 GAO findings. In 12 of the 15 cases, full corrective action has already been taken. Corrective action for the other three findings will be fully completed by the end of June. Moreover, steps are being taken to ensure that the conditions leading to the GAO's findings do not exist at the eight Reserve Banks that were not reviewed by the GAO.

The Federal Reserve's internal oversight of security is being focused to ensure that appropriate attention is given to the issues raised by the GAO. As we noted to the GAO, the Federal Reserve has for many years had a program of internal oversight based on independent operations review, financial examination, and audit staffs at both the Board and Reserve Banks. The Board's operations review and financial examination programs will scrutinize Fedwire security in these areas during 1990. Additionally, every Reserve Bank's internal audit function will perform a review of the Fedwire system, including security, to be completed by mid-year.

Two specific GAO findings relating to 1) the separation of duties between computer and network operators and 2) hardware redundancy on the "backbone" network linking the 12 Reserve Banks, may be due to some confusion regarding how Fedwire

security is implemented in these areas. The GAO report indicates that there should be a complete separation of duties between computer and network operators. Our view is that combining these functions has no detrimental effect on security and is industry practice. Adequate hardware redundancy already exists on the "backbone" communications network as part of a comprehensive and sound backup plan to provide quick recovery for the failure of any network component. This backup plan, which is tested quarterly and has been used successfully in production, has contributed to our network availability record of over 99.99 percent since the network was implemented in 1982. A detailed discussion of our response regarding network backup is appended to the GAO report.

The GAO also makes two systemwide recommendations. First, the GAO recommends that the Board require annual external reviews of Fedwire security. We agree that it is useful to engage the services of outside consultants to assess security. We believe, however, that such outside consultation can best be used when conditions support such a need, as opposed to regular annual consultations. The System has a history of employing outside technical consultants to assess security, as I already noted in the case of the development of the Federal Reserve's security safeguards. More recently, an outside assessment of Fedwire security has just been completed at the Federal Reserve Bank of New York. An outside consultant specializing in security performed a risk assessment of the Bank's Fedwire operations, including both automation and business areas. Use of a firm with specialized security expertise is intended, in part, to introduce

a view that is unconstrained by acceptance of traditional safeguards. It is a way to take a "fresh look" at what we do. The results of this security review will be shared among all the Federal Reserve Banks. In addition, the Board retains a public accounting firm each year to review a range of operations review and financial examination procedures. This year, the firm will review electronic data processing, including a review of security. We will continue to employ consultative services such as these when, based on management judgement, the circumstances warrant such input.

The GAO's second systemwide recommendation is that the Federal Reserve use both encryption and message authentication (known as MAC or message authentication codes) to enhance security. As noted earlier, nearly 100 percent of Fedwire links between Reserve Banks and depository institutions are already encrypted. Further, encryption of the "backbone" network will be completed by July 1990.

The Federal Reserve has made significant resource investments in studying the use of message authentication codes for Fedwire. These investments include active participation on American National Standards Institute study groups to develop bona fide national standards for message authentication and the complex process of key management that is a necessary part of a message authentication system. On a large network with a variety of endpoints, such as Fedwire, use of message authentication codes must take place in a manner consistent with approved technical standards for both authentication and management of authentication keys. Reliance on national standards is important

in order to avoid unique technical solutions that ultimately raise the costs of the depository institutions connected to Fedwire. Further, commercially available solutions that are cost effective for the range of depository institutions that use Fedwire must be available.

The first phase of a Federal Reserve effort to test emerging commercial message authentication code products that meet national standards has just been completed. These tests have not uncovered any technical impediments to the use of message authentication codes on Fedwire. With the results of this phase of our program to investigate message authentication codes complete, plans to adopt message authentication as an additional security enhancement for Fedwire are currently under review. Adoption of message authentication on Fedwire has my strong personal support.

I will now turn to the GAO recommendation that the Federal Reserve Board work with other central banks and bank supervisory authorities to ensure effective oversight and regulation of the S.W.I.F.T. system and similar systems that serve the international banking community. S.W.I.F.T. processes a large volume of payment orders that result in the transfer of very large sums between depository institutions, both domestically and abroad. S.W.I.F.T. differs from Fedwire and CHIPS, however, in the manner of settlement for these payment orders. In Fedwire, payment orders result in virtually instantaneous debits and credits on the books of the Reserve Banks without any independent action on the part of the sending or receiving bank. Similarly, CHIPS messages are settled

virtually automatically at the end of the day. Payment orders sent over S.W.I.F.T., on the other hand, must be settled independently of the S.W.I.F.T. system through correspondent accounts or through Fedwire or CHIPS transfers. In this regard, S.W.I.F.T. is only one of a number of different means that banks use to communicate payment orders. Payment orders may be transmitted telephonically or by data transmission, using a variety of providers of telecommunications services.

For any system used to transmit payment orders that may result in the transfer of large sums, however, a depository institution receiving the payment order should be responsible for verifying the authenticity and the content of the payment order before acting on it. A proposed new Article 4A to the Uniform Commercial Code makes it clear that depository institutions are liable if they act on unauthorized payment orders unless they use commercially reasonable security procedures. In some cases, a receiving bank may have sufficient confidence in the controls and the integrity of the system through which it receives payment orders to rely on this system's authentication and verification procedures. In other cases, a depository institution may wish to verify and authenticate payment orders by means of its own procedures.

We believe that the appropriate role of bank supervisors is to ensure that depository institutions maintain adequate authentication and verification procedures and that they do not rely on others to perform these critical functions without assuring themselves that these functions are performed adequately. Ordinarily, the supervisory focus should be on the

institution receiving a payment order rather than on a telecommunications system transmitting the order. Where a receiving depository institution relies on an authentication procedure provided by a telecommunications service provider, such as CHIPS, we may need to be able to examine the communications systems on which they rely in order to assure ourselves that depository institutions are not delegating these functions inappropriately. At the same time, however, we do not want to encourage depository institutions to delegate these functions to service providers merely because the service providers enjoy some degree of federal oversight. We will continue to monitor and evaluate bank reliance on telecommunications systems, including the S.W.I.F.T. system. When we discover problems stemming from banks' reliance on telecommunications systems we will take steps to strengthen our supervisory oversight and, where appropriate, coordinate any regulatory activities with supervisory authorities or central banks in other countries. We believe, however, that the principal responsibility to authenticate payment orders lies with the banks receiving these orders.

The Subcommittee has also asked for the Federal Reserve's broader perspective on the importance of technology in the future of the international financial marketplace. We expect a continuing and increasing reliance on automation and communications to provide secure, reliable, and efficient payment services. In our discussions with central bankers from other developed nations, it is evident that their approach to using advanced technologies for payment system applications is quite similar to that in the U.S. Most of the G-10 countries and

Switzerland have state-of-the-art computer systems with many of the features found in comparable U.S. banking systems. These systems rely on sophisticated computer systems, sound test procedures, and advanced recovery features designed to provide high availability. Generally, the same technology used in the U.S. for encryption, physical security, and access control is available in many other nations. As the cost effectiveness of automation improves, the use of advanced automation and communications technologies will continue to grow. Even today, the technology is available to link international financial markets around the clock.

The benefits and promise of this advanced technology, however, can only be achieved through its careful management. As payment systems become more reliant on sophisticated technology to deliver basic functions, the consequences of a systems failure or security breach is expanded significantly. We believe that close attention by senior management to automation planning, disaster recovery, and security is essential.

In conclusion, we are confident in the security architecture surrounding Fedwire and in this system's ability to provide high reliability in a secure environment. We appreciate the analysis conducted by the GAO and, in most cases, we agree with the findings and have moved quickly to correct the problems that have been identified. As I stated at the outset, the GAO's findings represent an opportunity to tighten the implementation of a security program that we believe is exceptionally sound.