THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

FINANCIAL SERVICES RISK ASSESSMENT REPORT

December 1997

TABLE OF CONTENTS

Page Number

EXECUTIVE SUMMARY ES-1

1.0 INTRODUCTION 1
- **1.1 Background** 1
- **1.2 Information Assurance and the Financial Services Infrastructure** 2
- **1.3 Objectives** 3
- **1.4 Scope** 6
- **1.5 Research Methodology** 7
- **1.6 Acknowledgments** 7

2.0 OVERVIEW OF THE FINANCIAL SERVICES INDUSTRY 8
- **2.1 Structure of the Financial Services Industry** 8
  - **2.1.1 Banks and Other Depository Institutions** 9
    - **2.1.1.1 Federal Reserve System** 9
    - **2.1.1.2 Commercial Banks** 10
  - **2.1.2 Investment-Related Companies** 11
    - **2.1.2.1 Underwriters/Investment Banks** 11
    - **2.1.2.2 Brokerages** 12
    - **2.1.2.3 Mutual Funds** 13
  - **2.1.3 Industry Utilities** 14
    - **2.1.3.1 Fednet** 15
    - **2.1.3.2 Other Payment Systems** 16
    - **2.1.3.3 Credit Card Systems** 17
    - **2.1.3.4 Exchanges** 18
    - **2.1.3.5 Clearing, Settlement, and Trust Utilities** 19
  - **2.1.4 Third-Party Processors and Other Services** 20
  - **2.1.5 Regulatory Structure and Reporting Requirements** 21

3.0 RISK MANAGEMENT 23
- **3.1 Definition of Risk** 23
- **3.2 Types of Risks** 24
- **3.3 Internal Risk Management Programs** 24
- **3.4 External Oversight and Regulation** 26
- **3.5 Threat Information and Risk Management** 27

4.0 RISK CONTROLS 28
- **4.1 Policy Risk Controls** 28
- **4.2 Personnel Risk Controls** 30
- **4.3 Information Systems Risk Controls** 31
  - **4.3.1 Access Controls** 32

TABLE OF CONTENTS

4.3.2 Applications Controls 33
4.3.3 Procedural Controls 33
4.3.4 Fraud Controls 34
4.3.5 Data Network Controls 35
4.3.6 Encryption 36
4.4 Telecommunications Risk Controls 37
4.5 Disaster Recovery Risk Controls 39

5.0 INDUSTRY TRENDS 42
5.1 Banking Trends 42
5.2 Investment-Related Company Trends 45
5.3 Emerging Services 47
5.4 New Technologies 50

6.0 CONCLUSIONS 52
6.1 Perceptions and Reality 52
6.2 Natural Disasters and Physical Attacks 54
6.3 Cyber Risks 55
6.4 Cyber Threats 57
6.5 Summary 58

7.0 RECOMMENDATIONS 59
7.1 Recommendations to the President 59
7.1.1 Threat Information Sharing 59
7.1.2 Personnel Background Investigations 59
7.1.3 Electronic Money and Commerce 59
7.1.4 NSTAC Membership 59
7.2 Recommendation to the Financial Services Industry 59

APPENDIX A-SUBGROUP MEMBERS A-1

EXECUTIVE SUMMARY

The United States' financial services infrastructure is arguably the finest in the world and plays an essential role in our ability to maintain a leading role in the world's economy. This report is the result of a 9-month study by the Information Assurance Task Force (IATF) of the President's National Security Telecommunications Advisory Committee (NSTAC) that included interviews and discussions with major institutions in all sectors of the financial services industry. The study found that at the national level the infrastructure is sufficiently protected and prepared to address a broad range of current threats, from natural disasters to electronic intrusions. However, there are security implications and potential vulnerabilities associated with the financial services dependence on a telecommunications infrastructure being subjected to deregulation, the integration of dissimilar information systems and networks resulting from mergers and acquisitions, and the introduction of web-based banking services.

The study focused on three objectives:

- Assess the security and robustness of the financial services infrastructure at the national level relative to the identified threats to its networks and information systems
- Determine the risks to the industry that derive from its dependence on the telecommunications infrastructure
- Examine the implications of trends regarding the industry's use of information systems and networks.

The most striking feature of how the industry approaches the protection of its networks and information systems is that security is considered an integral element of an overall program of risk management accountable to the most senior levels of an institution. This approach is long-established and factors into every investment decision. The approach also treats security measures as fundamental risk controls.

This report reviews the policy, personnel, information systems, telecommunications, and disaster recovery risk controls in place at major institutions. The extent of independent, mutually-reinforcing checks and balances in place within most critical systems and networks is unique to the financial services industry and provides its exceptional level of integrity and resilience. The study also found that most institutions have invested heavily to ensure the diversity of their telecommunications services, although local access remains a limitation in some areas.

All trends in banking, securities, and new technologies indicate that information systems and networks will continue to be the primary vehicles for innovation and competition, enabling money, value, and related commerce to move with increasing velocity.

The industry has paid for its reluctance to discuss security issues in open forums through perceptions fostered by the popular media that the situation is far worse than it is. The study determined that financial institutions were very aware of their threats, were committed to any

necessary investments in protection measures, and had extensive experience addressing natural and man-made disasters and infrastructure outages. These measures put successful cyber attacks beyond the scope of all but a concerted nation-state effort. Physical attacks remain the larger concern.

The report closes with several recommendations to the President and the financial services industry addressing threat information sharing, personnel background investigations, electronic money and commerce, and extensive screening for sensitive positions.

1.0 INTRODUCTION

This report documents the findings and recommendations of the assessment of the information assurance risks to the financial services industry by the Information Assurance Task Force (IATF) of the President's National Security Telecommunications Advisory Committee (NSTAC). In August 1996, a group of representatives of several NSTAC companies was formed to conduct this study. Representatives from the banking industry, the Federal Reserve Board, the Office of the Comptroller of the Currency, and the Department of the Treasury participated in the effort and provided technical advice to the IATF. The group members are listed in Appendix A. Mr. Steve Fabes, the Bank of America representative to the IATF, led this effort. The findings and recommendations of this report do not necessarily reflect the official views of the Treasury Department, Federal Reserve Board, or the Office of the Comptroller of the Currency.

1.1 Background

Information assurance, in the context of this report, is the protection of the networks and computers used in the nation's critical infrastructures against electronic attacks. The electronic web of computers and communications now touches virtually every aspect of American life. Both business and government have embraced computerization to boost productivity and efficiency. The widespread use of computers and networks exacts a price, however. Increased interconnectivity and interdependency of these systems cause us to be more vulnerable. As the most computerized and networked country in the world, the United States is the biggest potential target for attacks on its information systems. Headline articles from *USA Today* to *Time* magazine have painted frightening pictures of the prospects for an "electronic Pearl Harbor." Although the nation has avoided such a catastrophe, few would argue that the United States can afford to ignore the implications for national security of our move into an age of ubiquitous access to the information infrastructure.

The extent of the nation's vulnerability to attacks on its networks and information systems has become a major issue within Congress and the Executive branch. A series of hearings on "Security in Cyberspace" by the Senate Permanent Subcommittee on Investigations highlighted these concerns. John Deutch, the Director of Central Intelligence, remarked that, "My greatest concern is that hackers, terrorist organizations or other nations might use information warfare techniques as part of a coordinated attack to seriously disrupt electric power distribution, air traffic control, international commerce and deployed military forces."[1] Senator Jon Kyl (R-AZ) testified that, "Today, we do not have answers to even the simplest of questions. How vulnerable to attack is the national information infrastructure? How can government best engage various private sector elements on national security grounds?"[2]

---

[1] Hon. John M. Deutch, Director, Central Intelligence, Testimony Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, United States Senate, June 25, 1996.

[2] U.S. Senator Jon Kyl, *Testimony Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs*, United States Senate, July 16, 1996.

Composed of chief executives from 30 of the nation's leading telecommunications, computer, banking, and information services companies, NSTAC has provided an independent industry voice to the President on critical issues of networks as they support national security and emergency preparedness since its creation in 1982. NSTAC is unique in providing the President with a direct conduit for advice and input from industry in one of the critical infrastructures.

In January 1995, the Director of the National Security Agency briefed the NSTAC on threats to U.S. information systems and the need to improve the security of critical national infrastructures. The NSTAC principals discussed those issues and subsequently drafted a letter to the President in March of that year stating that, "[t]he integrity of the Nation's information systems, both government and public, are increasingly at risk from intrusion and attack [and that] other national infrastructures [such as finance, air traffic control, power, etc.,] also depend on reliable and secure information systems, and could be at risk."[3]

The President replied to the NSTAC letter in July 1995, stating that he would "welcome NSTAC's continuing effort to work with the Administration to counter threats to our Nation's information and telecommunications system."[4] The President further asked, "the NSTAC principals-with input from the full range of users of the NII-to provide me with your assessment of national security and emergency preparedness requirements for our rapidly evolving information environment."[5] The NSTAC formed the IATF to address these issues.

The IATF determined that three infrastructures-electric power, financial services, and transportation-were most dependent on public and private telecommunications and information systems for essential operations. The IATF's study of information assurance in the electric power industry was conducted between March and September 1996, and its report was approved by the NSTAC principals in March 1997. The transportation risk assessment effort is scheduled to be completed before NSTAC XX.

1.2 Information Assurance and the Financial Services Infrastructure

Of all the critical infrastructures, telecommunications and financial services clearly are the most dependent upon networks and information systems. Indeed, the financial services industry may be the telecommunications industry's most demanding customer. The Minority Staff statement before the Senate's "Security in Cyberspace" hearings outlines the extent of the interdependence of the nation's economy and the telecommunications and information systems infrastructure, often referred to collectively as the National Information Infrastructure (NII):

> Much of the way money is accounted for, handled, and exchanged is now done via the NII. Salaries are directly deposited into bank accounts by electronic funds transfers. Automated teller machines ("ATMs") deposit funds, withdraw funds, and make payments.

---

[3] Letter from Mr. William Esrey, Sprint Corporation and Chair of the NSTAC, to the President of the United States, dated March 20, 1995.

[4] Letter from the President of the United States to the NSTAC, dated July 7, 1995.

[5] Ibid.

> When payment is made for merchandise with debit cards and credit cards, transactions are verified using the public switched network. Much of our national economy also depends on the NII. The vast majority of transactions conducted by banks and other financial institutions are done via electronic funds transfers. Over $2 trillion is sent by international wire transfers every day. In addition, most securities transactions are conducted via computerized systems.[6]

As described in the Department of the Treasury's report, *An Introduction to Electronic Money Issues*, "the convergence of computing and telecommunications is fundamentally changing the character of traditional money and related financial activities and setting the stage for even greater changes in the years ahead."[7] Citicorp's chief executive officer, John Reed, recently commented that he expected banking eventually to become "a little bit of application code in a smart network."[8]

The increasingly interconnected nature of the financial services and telecommunications infrastructures has profound security implications. For example, vulnerabilities in one network can often expose other systems connected with it to the same risks. As NSTAC's Network Security Information Exchange observed in its 1995 report, *An Assessment of the Risk to the Security of Public Networks*, "while reliance on the public network is growing, protection measures are not keeping pace with new and emerging vulnerabilities."[9] In particular, there is a concern that the increased exposure to network attacks, combined with the growing dependence on network services, creates the potential for new systemic risks that go far beyond the scope of individual institutions' traditional risk management mechanisms.

1.3 Objectives

The study group identified the following three primary objectives for its effort:

- Assess the security and robustness of the financial services infrastructure at the national level relative to the identified threats to its networks and information systems
- Determine the risks to the financial services industry that derive from its dependence on information technology and the telecommunications infrastructure
- Examine the implications of trends regarding the industry's use of information systems and networks.

First, the study attempts to provide an independent assessment of the risk of attacks on current financial information systems and networks causing a catastrophic collapse of the nation's

---

6 Minority Staff Statement, U.S. Senate Permanent Subcommittee on Investigations (Minority Staff) Hearings on Security in Cyberspace, June 5, 1996.

7 U.S. Department of the Treasury, *An Introduction to Electronic Money Issues*, prepared for the conference, "Toward Electronic Money and Banking: The Role of Government," September 19-20, 1996.

8 Martin Mayer, *The Bankers: The Next Generation*, New York: Truman Talley Books/Dutton, 1997.

9 Network Security Information Exchange, *An Assessment of the Risk to the Security of Public Networks*, 1995.

economy. Although fiction writers can describe nightmarish scenarios of computer viruses disabling stock exchanges and hackers taking down vital electronic funds transfer networks, industry and government need to deal with facts. An effective assessment of the risk of systemic failure requires an informed examination of both the technical and the business implications of potential disruptions.

Second, based on NSTAC's continuing investigations into the vulnerabilities of public networks and information systems, the study considers the risks to the financial services industry that derive from its dependence on information technology and the telecommunications infrastructure. With the volume of funds handled each day through the nation's financial networks, reliable telecommunications services are essential. What are the effects of extensive disruptions of public networks? Natural disasters have provided institutions in some regions with plenty of experience in dealing with major outages, but the rise of the cyber threat introduces the potential for major man-made disruptions.

The reliance on public and private network services also creates the potential for disruptions through the use of tools and techniques seen in attacks on other information systems. These attacks can be staged from outside an institution, through remote-access lines, Internet gateways, and other interfaces to public networks or trusted third parties, or from inside, by disgruntled or compromised employees or contractors. Like other organizations, financial institutions rely on a combination of access controls, process controls, and other measures to deal with these risks. With the proliferation of information technology and a shift to shorter product development cycles, maintaining these controls can be a considerable technical and organizational challenge.

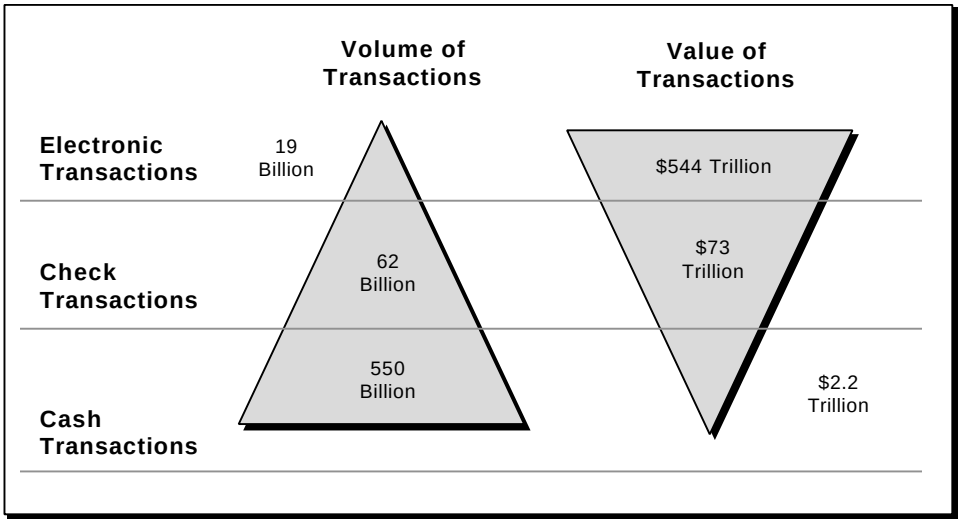
Finally, the study examines the implications of trends in how the financial services industry is using information systems and networks. Banks and other financial institutions are undergoing a generation change in information technology. Proprietary, relatively isolated, and highly protected networks centered on mainframe systems are being augmented and gradually replaced by intranets that integrate a complex array of desktops, servers, applications, and local and wide area networks. Competition is driving innovation within the industry. A rush to deploy new technology and innovative products and services raises questions about the extent to which security measures and practices are considered and implemented.

The automation of payments and market systems has enabled a tremendous increase in the volume and velocity of financial transactions. In the early 1970s, the New York Stock Exchange closed every Wednesday to clear backlogs from an average daily trading volume of 11 million shares. Today, the systems of the Securities Industry Automation Corporation (SIAC) routinely handle 500 million share/days with no interruption to exchange operations.[10] Clearing and settlement processes have been cut from 1 week to 3 days and are moving towards the goal of same-day or even real-time settlement.

[10] *SIAC Corporate Overview, 1997.*

Although cash and paper check transactions still outnumber electronic transactions, electronic transactions account for virtually all large-value payments and exchanges (see Figure 1-1). The increasing use of credit and debit cards, enabled through ever-expanding networks of point-of-sale terminals, suggests that electronic transactions will account for more and more low-value payments. Even cash transaction trends have been significantly affected by the fact that ATMs provide many people with their primary access to cash.

Figure 1-1. The Volume and Value of Electronic, Check, and Cash Payments in the United States, 1995



Source: National Automated Clearing House Association, 1995

Individual and institutional investors now can move money between different sectors very quickly. Customers can redeem stocks or shift funds from one mutual fund company to another with little delay. Securities firms offer cash management accounts that allow customers to write checks and get cash at ATMs. As a result, bank demand deposits, which traditionally have been viewed as the most liquid and accessible form of funds next to cash, represent a shrinking share of financial assets. The ease and speed with which funds can be moved in and among nonbank accounts disguise the fact that these accounts are not Federal Deposit Insurance Corporation (FDIC) insured and are vulnerable to changes in market and economic conditions. In this environment, disruptions to financial systems can have more profound and more widespread effects than ever experienced before.

In the midst of these developments, the introduction of electronic commerce and electronic money further increases the complexity and interdependence of the elements of the financial services infrastructure.

1.4 Scope

Because NSTAC is chartered to address national-level issues, this study limited its scope to institutions and systems that could have broad impacts in the event of disruption, compromise, or degradation. Although tens of thousands of firms compose the financial services industry, the

bulk of financial assets and the greatest volumes of financial transactions are handled by a relatively small number of institutions: large national or money center banks; leading market makers in securities; the largest third-party processors; and the primary industry utilities, including the exchange, clearing, settlement, and payments systems. All of these are characterized by the large number and high total value of transactions processed.

The clearing, settlement, and payments systems have long been recognized as the vital core of the financial services industry. As Gerald Corrigan, then-president of the Federal Reserve Bank of New York put it,

> Default in one of these systems has the potential to seriously and adversely affect all other direct and indirect participants in the system, even those that are far removed from the initial source of the problem. Unlike many other types of financial problems, a major disruption in one of these systems can occur suddenly and can spread rapidly. . . .[11]

Federal Reserve Chairman Alan Greenspan recently testified that such disruptions "[C]an easily have global implications. Fedwire, CHIPS, and the specialized depositories and clearinghouses for securities and other financial instruments are crucial to the integrity and stability not only of our financial markets and economy, but those of the world. Similarly, adverse developments in transfer systems in London, Tokyo, Singapore and a host of other centers could rapidly be transferred here, given the financial interrelationships among the individual trading nations."[12] This issue has been a concern for many of the world's central banks.

In 1990, the Bank for International Settlements issued a landmark report that established minimum guidelines for managing settlement risk on large-value payment systems.[13] Known as the Lamfalussy Report, it provided a benchmark for managing risk in domestic and international netting arrangements. Even systems handling smaller value payments-such as credit card associations-have used the Lamfalussy standards to evaluate their own risk protections.

That the concentration of assets and transactions in these systems qualifies them as critical national assets is undeniable. This study does not, however, make any judgment about whether this concentration is appropriate from an economic or security standpoint. In general, the study group found U.S. financial institutions were very aware of their criticality and potential impacts on their customers and others in the industry and the national economy.

1.5 Research Methodology

---

11 Martin Mayer, op. cit., p. 354.

12 Statement by Alan Greenspan, Chairman, Board of Governors of the Federal Reserve System, before the *Subcommittee on Capital Markets, Securities, and Government-Sponsored Enterprises of the Committee on Banking and Financial Services*, U.S. House of Representatives, March 19, 1997.

13 Bank for International Settlements (BIS*), Report of the Committee on Interbank Netting Schemes of the Central Banks of the Group of Ten Countries* (1990).

Confidential interviews with representative institutions in the industry were the primary means of research for this study. From December 1996 to April 1997, interview teams visited more than 20 firms, including money center banks, securities firms, credit card associations, third-party processors, and payment and industry utilities. The interviews, which generally lasted 3 to 4 hours, covered issues ranging from network architectures and security technologies to policies, management reviews, and hiring practices. Without identifying the firms that participated, the study group would like to acknowledge their outstanding support and exceptional candor in discussing sensitive and often highly proprietary matters. This candor was elicited by the interview team's commitment to those interviewed that neither they nor their companies would be identified as the source of any information contained in the report.

To augment the interview data, the study group contacted a number of industry associations to inform them of the effort and solicit their comments and suggestions. These associations included the following:

- The American Bankers Association
- The Bankers Roundtable
- National Automated Clearing House Association
- Electronic Funds Transfer Association
- Securities Industry Association
- Information Industry Association.

Their help in identifying contacts within the industry and providing background material was invaluable. The staff of the American Bankers Association in particular offered exceptional support. The study group also contacted the Federal regulatory agencies responsible for oversight and supervision of the industry, including the Federal Reserve Board, the Office of the Comptroller of the Currency (OCC), and the Securities and Exchange Commission. Finally, the group coordinated its efforts with those of the President's Commission on Critical Infrastructure Protection (PCCIP) and the Infrastructure Protection Task Force (IPTF).

1.6 Acknowledgments

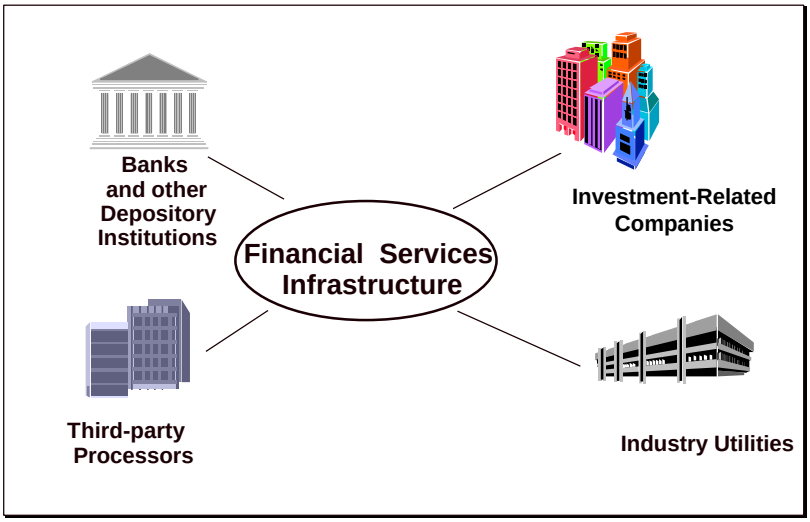
The IATF and Steve Fabes, Bank of America and Chair of the Financial Services Risk Assessment Subgroup, would like to convey their appreciation and respect for the subgroup members and all other contributors to this report. Without their significant investment of time, expertise, and other resources, this report would not have been possible. Appendix A lists the subgroup members and other contributors to the report.

2.0 OVERVIEW OF THE FINANCIAL SERVICES INDUSTRY

The U.S. financial services industry is a complex web of interrelated organizations and systems through which instruments of monetary value are processed. The term "financial services industry" is somewhat problematic, because historically there have been significant differences and even stringent regulatory barriers between banks, investment firms, and other financial institutions. Competition for customer funds and ongoing deregulatory efforts, however, are

eliminating many of these distinctions and lowering some of the regulatory barriers. As described in the Introduction, retail and commercial customers can now move money between, and obtain similar services from, institutions in different sectors, so that it is now possible to refer meaningfully to the financial services industry as an integrated infrastructure. As Martin Mayer has commented, today, "everybody wants to be a Financial Services Institution."[14]

Figure 2-1. Financial Services Industry Categories



2.1 Structure of the Financial Services Industry

For the purposes of this study, the financial services industry is defined as follows:

- Banks and other depository institutions
- Investment-Related companies
- Industry utilities
- Third-party processors and other servicers.

Insurance, consumer finance, and mortgage companies were excluded because disruptions to their networks and information systems likely would have less immediate and widespread effects at a national level. As of September 1996, U.S. banks hold approximately $4.4 trillion of the domestic financial assets outstanding, and investment companies and other private nonbank institutions hold about $13.4 trillion.[15]

2.1.1 Banks and Other Depository Institutions

[14] Martin Mayer, op. cit., p. 185.

[15] "Statistical Information on the Financial Services Industry," American Bankers Association, Seventh Edition, 1996.

Over time, banks and other depository institutions-including savings and loan associations, credit unions, and thrifts-have evolved to perform the following functions:

- Hold and provide access to deposits
- Provide loans
- Enable funds transfer
- Promote savings
- Facilitate economic growth.

In addition, the Federal Reserve System acts as the central bank for the United States. This study limited its consideration of banks to the largest money center banks, those which hold assets on the order of $100 billion or more and which play pivotal roles, both in terms of the customer base they serve and as major participants in both regional and international markets.

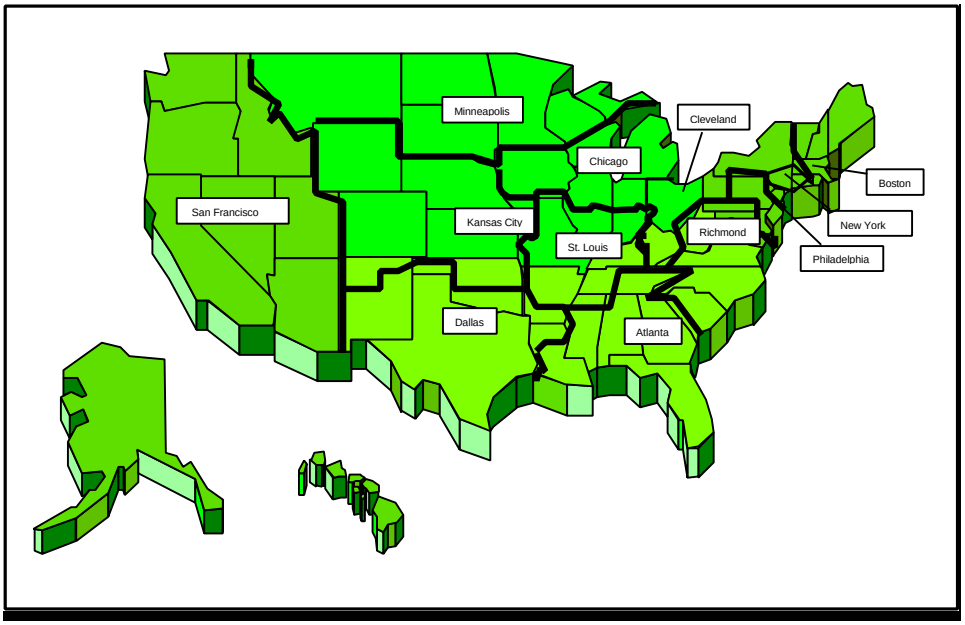
2.1.1.1 Federal Reserve System

In 1913, Congress established the Federal Reserve System as the central banking system of the United States. The central bank is perhaps the most important banking institution of all and exists in some form in every country. The central bank deals with other banks rather than with the public and handles the reserve balances of depository institutions, provides clearing services, and extends emergency credit facilities for depository institutions. Central banks also issue currency and control the money supply, interest rates, and foreign exchange.

In the United States, the Federal Reserve banks are owned by private member banks but supervised by the Board of Governors, which is appointed by the President of the United States with the advice and consent of the U.S. Senate. For purposes of administering the Federal Reserve System, the country is divided into 12 districts, each of which is serviced by a Federal Reserve Bank. Each of the 12 Federal Reserve Banks (shown in Figure 2-2) is a corporation organized and operated for public service. The capital stock of these banks is owned by the private member banks.

The mission of the Federal Reserve is to set monetary policy; maintain the stability of the financial system and contain systemic risk that may arise in the financial markets; provide services to financial institutions and other government agencies; and supervise and regulate banks and bank-holding companies. The study group was primarily interested in the services provided by the Federal Reserve to financial institutions.

Figure 2-2. United States Federal Reserve Districts



The Federal Reserve provides check-clearing and processing and electronic transfer of funds and government securities between financial institutions. The Federal Reserve also distributes and receives Federal Reserve notes (paper money) and issues and redeems Government securities for the Department of the Treasury.

2.1.1.2 Commercial Banks

Commercial banks have the largest amount of assets of any depository institutions. Commercial banks finance credit needs, collect deposits, transfer funds, issue letters of credit, serve as trustees for individuals or corporations, act as agents in the purchase and sale of securities, and disseminate economic information. The deposit accounts at most commercial banks are backed by the FDIC. The FDIC provides deposit insurance to banks if they meet the FDIC requirements, submit to Federal supervision, and pay an annual assessment based on their total deposits. Currently, individual depositors are insured up to the legal limit of $100,000 per institution.[16]

The top 10 commercial money center banks hold over 33 percent of the total assets controlled by banks. As of June 30, 1996, the top five commercial banks in the United States ranked by total assets are Chase (Chemical), Citibank, Bank of America, NationsBank, and Morgan Guaranty Trust (see figure 2-3).[17] Banks often enter into corresponding bank relationships in which a bank regularly performs services (e.g., carrying deposit balances for banks in another city) for another bank in a location or market to which the other does not have direct access.

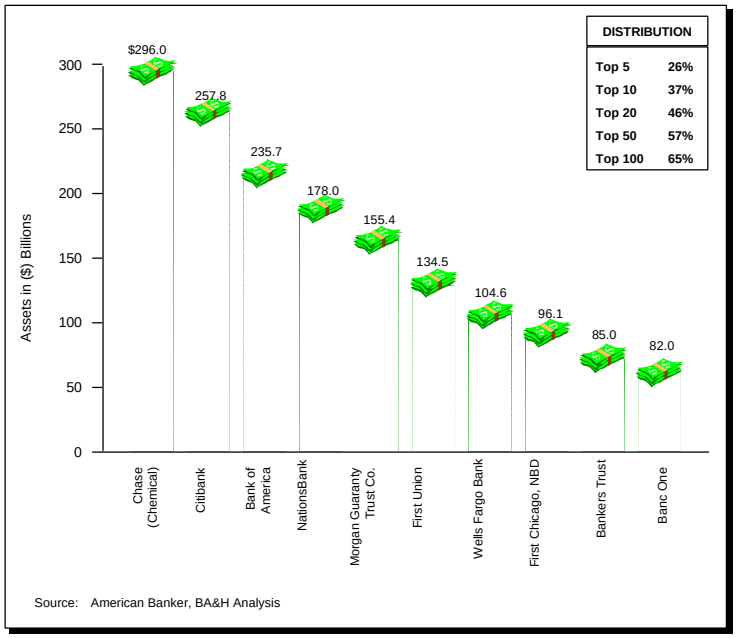
---

16 *FDIC website (www.fdic.gov).*

17 "Top 300 U.S. Commercial Banks in Total Assets." *American Banker*, October 28, 1996.

Savings banks, savings and loans association, and credit unions are broadly referred to as "other depository institutions." Historically, nonbank depositories usually service households rather than businesses, and deposits are usually held as savings or time deposits. Credit unions represent the most significant player among the nonbank depositories. As of January 1996, the 11,687 federally insured credit unions had more than 60 million members and $306.2 billion in assets.[18]

Figure 2-3. Top 10 U.S. Commercial Banks Ranked byTotal Assets, 1996



2.1.2 Investment-Related Companies

Many companies provide a variety of services to individual and institutional investors, acting as an intermediary in market trades and pooling investments by a large group of customers through mutual funds. Some companies specialize in only one aspect of investment activities; others, most notably Merrill Lynch, compete in all three of the primary types of investment activities: underwriting, brokerage, and mutual funds. Competition among the various investment companies is fierce.

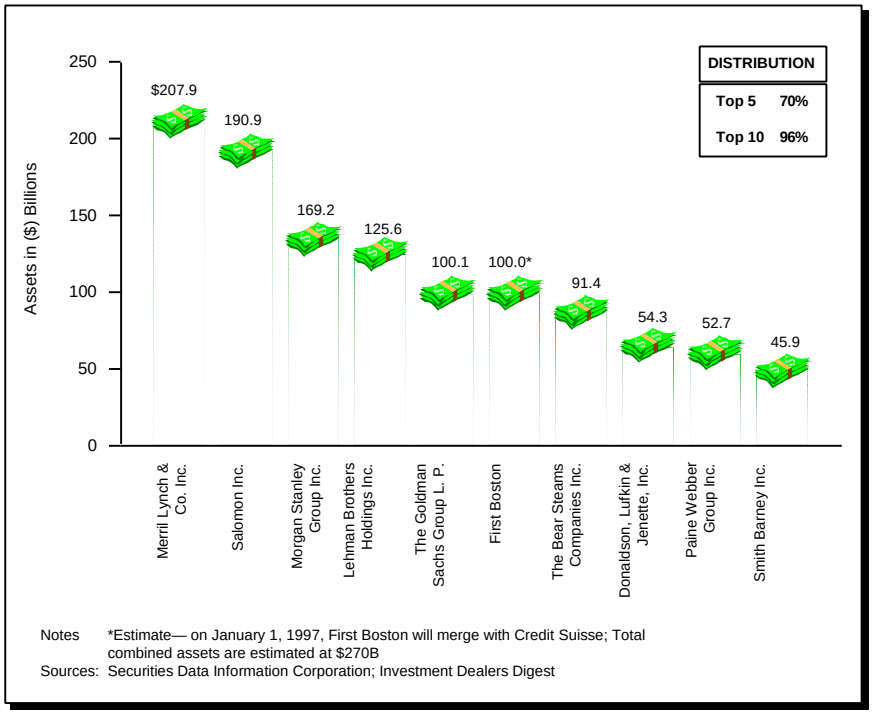
2.1.2.1 Underwriters/Investment Banks

Unlike commercial banks, investment banks are not depository institutions. Rather, investment banks finance investments by both private enterprises and governments at all levels through the underwriting of stocks and bond issues. In addition, investment banks market a variety of stock and bond issues, arrange mergers, and coordinate initial public offerings (IPO) of

[18] National Credit Union Association web page (www.ncua.gov).

stocks. The majority of investment banks also maintain brokerage operations. Investment banking is still an exclusive club: in the United States, the top five investment banks control 70 percent of the market (see Figure 2-4).

Figure 2-4. Top U.S. Investment Banks Ranked by Total Assets, 1996

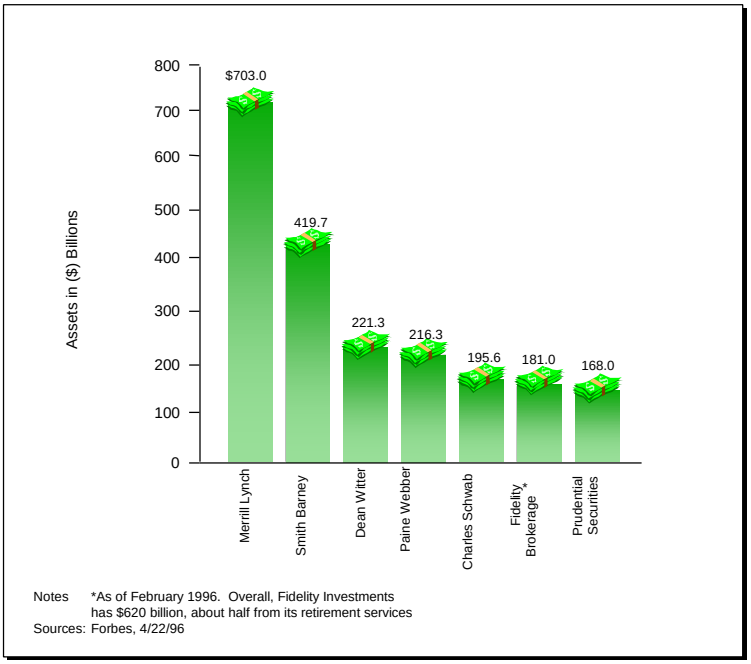


2.1.2.2 Brokerages

Brokerages act as intermediaries between investors and securities or commodities markets. Brokerages are generally overseen by the self-regulatory organizations (SROs) of which they are members, the Securities and Exchange Commission (SEC), the Commodities Futures Trading Commission (CFTC), and the States in which the brokerage is conducting business.[19] Brokerages range from full-service firms that place trades, perform research, and advise clients to discount brokerages that offer clients fewer services, usually at reduced fees. Brokerages are investing heavily in technology and developing new products, services, and delivery systems to retain customers and attract new ones. As illustrated in Figure 2-5, the top five brokerages in the United States are Merrill Lynch, Smith Barney, Dean Witter, Paine Webber, and Charles Schwab.

Figure 2-5. Top U.S. Brokerages Ranked by Total Assets, 1996

[19] Within the securities and commodities industries, SROs promulgate "industry rules," which are generally designed to ensure fair, efficient, and ethical practices in the securities and commodities futures industries. SROs include the DTC, NSCC, all the national securities and commodities exchanges, and the National Association of Securities Dealers (NASD), which represents all firms operating in the over-the-counter market. The SEC and CFTC must approve SRO rules before they can become effective. In addition, the SEC and CFTC have promulgated rules under their respective Acts which govern market practices.



2.1.2.3 Mutual Funds

A mutual fund brings together money from many people and invests it in stocks, bonds, or other securities according to the fund's investment goal. A portfolio manager is employed by the mutual fund to pursue the fund's goal, which may include maximizing long-term return or providing a reliable source of current investment income. In return for investment management and other services, the fund charges a variety of fees. Mutual funds are registered with and regulated by the SEC. Assets held in mutual funds exceed $3.7 trillion and have experienced tremendous growth during the past decade.[20] It is important to note that although some funds now provide access to a variety of services, including cash withdrawals at ATMs, debit cards, and check-writing, investments in mutual funds are not insured by the Government like certain bank demand deposit accounts. Twenty-five mutual fund companies dominate the market, with the top five companies—Fidelity, Vanguard, Merrill Lynch, American, and Franklin—representing 33 percent of the market.[21]

2.1.3 Industry Utilities

This study defined financial services utilities as the institutions that provide a common means for the transfer, clearing, and settlement of funds, securities, and other financial instruments, as well as the exchange of other types of financial information. Although cash and check transactions still account for the largest number of financial transactions, electronic

[20] Investment Company Institute.

[21] Ibid.

transactions, through wire transfers, interbank payment systems, automated clearing houses, and clearing and settlement systems for securities and other investments, dwarf paper transactions in terms of total value. Table 2-1 illustrates the tremendous volume and value handled by these utilities.

With the exception of Fednet, most of these utilities are not-for-profit companies held jointly by their members and funded through membership dues and transaction fees. In the securities and futures business, these utilities are designated as SROs; but even in the banking sector, government regulators recognize the considerable role in self-policing and standards-setting played by clearing houses, credit card associations, and other such utilities. This section describes the leading financial services utilities in the United States.

Table 2-1. Annual Transaction Volumes/Values, 1996[22]

Organization	Annual Transaction Volume (In Millions)	Annual Transaction Value (In $Trillions)
CHIPS	53.4	$331.5
Fednet/Fedwire funds transfer	82.0	$246.0
Fednet/Book-entry securities	13.0	$162.0
The Depository Trust Company (1995)	135.7	$50.2
Government Securities Clearing Corporation	3.0	$25.0
National Securities Clearing Corporation	140.0	$11.0
Fednet/ACH	2,800.0	$10.0
Options Clearing Corporation	200.0	$2.8
Private ACH	1,100.0	$2.0
VisaNet	2,250.0	$0.937

2.1.3.1 Fednet

Fednet is a unified communications network that connects all 12 of the Federal Reserve banks nationwide. Fednet provides three primary services to the financial services industry:

- Fedwire funds transfer, the real-time gross settlement funds transfer network among banks and other depository institutions

[22] CHIPS, Federal Reserve Board, DTC, Visa, OCC, the National Automated Clearing House Association, and BA&H analysis.

- Fedwire book-entry securities transfer, the real-time delivery system for the sale of government securities[23]

- Automated clearing house.

Fedwire is the primary national network for funds transfer between banks. Approximately 11,000 institutions use Fedwire, accessing it over dedicated and dial-up lines. Transfers initiated on Fedwire are irrevocable upon receipt and are settled immediately. Fedwire funds transfer and dollar volumes have grown rapidly. Between 1987 and 1996, the number of funds transfers originated increased 57 percent, from 52.4 million to 82 million. Concurrently, annual dollar volumes increased 62 percent, from $152 trillion to $246 trillion. By year-end 1997, the Fedwire funds transfer service will expand its hours of operation from 10 to 18 hours. The average value of a Fedwire funds transfer is over $3 million.[24]

Fedwire's book-entry securities transfer application allows depository institutions to transfer U.S. government securities for themselves and customers, such as the primary dealers. In 1996, the Federal Reserve transferred 13 million book-entry securities, valued at over $162 trillion.[25] This capability has enabled the Federal Reserve to largely replace paper U.S. government and agency securities with electronic book-entries. The book-entry securities transfers are processed individually, similar to Fedwire funds transfers. When the Federal Reserve receives a request to transfer a security, it first determines that the security is held in safekeeping for the requesting institution and then withdraws the security from the sending institution's safekeeping account. The Fed then electronically credits the proceeds of the sale to the account of the depository institution, deposits the book-entry security into the safekeeping account of the receiving institution, and electronically debits that institution's account for the purchase price. The Federal Reserve guarantees all payments to institutions sending book-entry securities transfers.

The automated clearing house (ACH) process was developed in the early 1970s as a more efficient alternative to the traditional paper-based check clearing house process. ACH transactions include direct bill payments by consumers and businesses and direct deposits of payrolls, dividends, pensions, and benefits. The Federal Reserve provides ACH services to all depository institutions. Several private institutions—the New York Clearing House Association (NYCHA), Visa, and the Arizona and Hawaii Automated Clearing Houses—also provide ACH services; but the Federal Reserve accounts for most of the ACH transactions by dollar volume and value. The private ACH operators rely on the Federal Reserve to handle ACH transactions with institutions outside their customer group. The average cost of an ACH transaction has fallen from 12 cents to less than 1 cent as a result of improved information technology and competition.

---

[23] Book entry securities are securities that are not represented by paper certificates; rather, they are electronic records.

[24] Federal Reserve Board.

[25] Federal Reserve Board.

From 1986 to 1996, ACH transaction volumes increased 420 percent, from 750 million transactions to 3.9 billion transactions. During that same time, total dollar volume increased 450 percent, from $2.2 trillion to $12 trillion. In 1996, the Federal Reserve processed 2.8 billion ACH payments with a value of $10 trillion.[26]

Unlike Fedwire funds transfers, which are processed individually and settled immediately at the time of processing, ACH payments are transmitted electronically in batches to a Federal Reserve processing center by a depository institution. These transfers are generally processed 1 or 2 days before settlement date and are delivered to receiving depository institutions several times a day as they are processed.

2.1.3.2 Other Payment Systems

Clearing House Interbank Payments System

The Clearing House Interbank Payments System (CHIPS), owned and operated by the NYCHA, is an electronic system for interbank transfer and settlement. In 1995, CHIPS transmitted more than $330 trillion, including 90 percent of all international U.S. dollar payments, which themselves include billions in foreign exchange and Eurodollar settlements made in U.S. dollars. CHIPS participants include over 100 banks, both U.S.-based and the U.S. branches of most of the largest international banks. Although CHIPS payments are made in U.S. dollars, the system serves as the primary clearing system for foreign exchange.

The 104 CHIPS participants are linked by dedicated, high-speed diversified data communication lines to the CHIPS data center. At the close of business, end-of-day reports are distributed to each participant. If there are no abnormal notices of settlement, each participant that is in a debit position sends its settlement obligation via Fedwire to the CHIPS settlement account at the Federal Reserve Bank of New York. When all debtor settling participants have sent their obligations, the NYCH, as agent of all settling participants, will send Fedwires from the settlement account to the creditor participants in the amount of their aggregate net credit positions. When all Fedwires to the creditor settling participants are completed, settlement is complete. CHIPS normally completes its settlement process by 5:30 p.m. Eastern Standard Time.

Society for Worldwide Interbank Financial Telecommunications

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) was formed in 1973 to provide members with a secure, cost-effective international payment message system. Members include financial institutions, stock exchanges, brokers, clearing houses, and investment management institutions. The primary uses of SWIFT include transmitting and routing financial messages. These messages are instructions between banks and other institutions regarding payments and transfers, not payments themselves. A significant amount of traffic over SWIFT relates to corresponding payments made through CHIPS. SWIFT transfers approximately 2.8 million messages per day.[27]

[26] Federal Reserve Board, National Automated Clearing House Association.

[27] SWIFT.

2.1.3.3 Credit Card Systems

Credit cards represent a $1.2 trillion dollar industry with more than 1 billion credit cards issued.[28] There are two types of credit cards issued in the United States: bank cards and private cards. Visa and MasterCard are the two bank card associations. Their various services include providing a uniform way of branding cards regardless of the issuing institution, providing a consistent set of services to merchants that honor the card, and routing of authorization requests. Visa and MasterCard are owned by their participating banks and depository institutions, which actually issue the cards and handle billing and payments on their accounts. Private card issuers such as American Express and Discover handle all these functions themselves.

Credit card transactions represent an enormous volume of traffic in the financial services infrastructure. Point-of-sale terminals in millions of locations worldwide generate thousands of requests for authorization of credit each second. A combination of dedicated and dial-up links ties these terminals into a complex network of third-party processors, card associations, and acquiring (i.e., the merchant's) and issuing (the consumer's) banks. Massive databases of account histories and profiles, combined in some cases with sophisticated fraud analysis tools, work in tight synchronization to allow authorization requests to be processed in seconds.

The credit card industry has experienced significant increases in fraud, with most of the loss at the expense of the card issuers. From 1987 to 1992, annual losses climbed from $150 million to over $600 million.[29] Consumers, however, are protected by Federal Reserve Regulation E, which limits credit card holder liability for fraudulent charges to $50.

2.1.3.4 Exchanges

Exchanges provide a place or facilities for bringing together buyers and sellers of securities or commodities. Stocks, bonds, commodities, futures, and derivatives are the fundamental items currently traded in the markets today.

Equities Exchanges

A stock or equities exchange is a market where trading in securities is conducted on an organized basis. Securities are often bought and sold in a number of different markets. The largest securities markets are the New York Stock Exchange, the National Association of Securities Dealers' Automated Quotation System (NASDAQ) stock market, the American Stock Exchange (AMEX), and the Chicago Board Options Exchange (CBOE). Structurally, the New York, Chicago, and American exchanges are very similar to each other, selling securities on the floor of the exchange in an open auction.

---

[28] *Hoover's Handbook of American Business,* 1996.

[29] Bankers Roundtable, *Banking's Role in Tomorrow's Payment Systems,* Volume I, 1994.

NASDAQ is an electronic communications network that consolidates the quotations of multiple dealers which are displayed real-time to its members. The system enables dealers to update displayed quotes. NASDAQ offers services that allow electronic trading, however, most order entry and execution for NASDAQ securities still occur by telephone.
Like the traditional exchanges, the NASDAQ is owned and self-regulated by its membership—the National Association of Securities Dealers—with oversight from the SEC.

In addition to the NYSE, AMEX, and NASDAQ, there are regional exchanges in Philadelphia, Chicago, Boston, and San Francisco. In 1994, over 162 billion shares worth over $4.2 trillion traded between the NYSE AMEX, NASDAQ, and the regional exchanges. The NASDAQ is the most active of the markets, trading over 138 billion shares in 1996 valued at over $3.3 trillion, while the New York Stock Exchange traded 104 billion shares.[30]

Futures Exchanges

Futures are legally binding agreements to buy or sell a commodity in the future. These agreements are standardized according to the quality, quantity, delivery, time, and location for each commodity. Futures have experienced tremendous growth since the 1970s. Futures contracts are available for interest rates, stock indexes, manufactured and processed products (e.g., corn, pork bellies), precious metals, and foreign currency.

The Chicago Board of Trade (CBOT) is the world leader for commodities, securities, and financial instruments futures, and options on futures. The CBOT has more than 3,600 members who executed 210 million trades in 1995. The New York Mercantile Exchange (NYMEX) handles trades on futures contracts such as crude oil, heating oil, unleaded gasoline, propane and natural gas, as well as in platinum and palladium. In the first quarter of 1996, the NYMEX energy complex traded an average of nearly 243 million crude oil equivalent barrels per day, which represents about three times daily world oil production—and nearly 10 times daily OPEC production, with an annual value well in excess of $1 trillion.[31]

2.1.3.5 Clearing, Settlement, and Trust Utilities

Exchanges provide a place and facilities for trading. Clearing and settlement is the processing of transactions after the trades are made. Clearing confirms the identity and quantity of the instrument or contract being bought and sold, the price and date of the trade, and the identity of the buyer and seller. Settlement is the fulfillment of the trade.

In the securities markets, settlement is the delivery of stocks or bonds to the buyer and the corresponding payment to the seller. In futures and options markets, settlement takes place in a variety of ways, from physical delivery of goods at a specified place and time to transfer of the terms of the contract to a subsequent contract. These steps are essential to the market

30 *1996 NASDAQ Fact Book.*

31 New York Mercantile Exchange (www.nymex.com).

mechanism: failure in a utility performing the settlement function would likely force a suspension of trading on the markets it supports.

Several clearing organizations help mitigate settlement risk by netting the delivery of payments and securities. The National Securities Clearing Corporation (NSCC) is owned by the New York and American stock exchanges and the NASD. The NSCC processes most of the equity transactions in the United States. It interfaces with The Depository Trust Company (see below). The Government Securities Clearing Corporation (GSCC) is affiliated with the NSCC and performs similar functions for exchanges of government securities.

In the futures markets, the Board of Trade Clearing Corporation (BOTCC) supports the Chicago Board of Trade, where a majority of futures are traded in the United States. The Options Clearing Corporation supports all of the options exchanges in the United States.

The Depository Trust Company

The Depository Trust Company (DTC) settles securities trades and is a custodian for its participant banks, broker-dealers, and trust companies. It is the world's largest securities depository with more than $12 trillion worth of securities in custody.[32] In 1996, DTC participants delivered $50.2 trillion of securities through the depository's book-entry system (i.e., electronic records of ownership).

DTC places securities in its nominee name in a central securities record-keeping system to facilitate transfers and settlement of securities transactions, such as transfers and pledges. This process is called immobilization. Most securities are exchanged as book entries, not paper certificates. DTC is jointly owned by its participants-the New York Stock Exchange, the American Stock Exchange, the National Association of Securities Dealers, and its clearing banks and broker-dealers. It is operated by separate management and has an independent board of directors. It is a limited purpose trust company, and a "clearing corporation" within the meaning of the New York Commercial Code and a "clearing agency" registered under Section 17A of the Securities and Exchange Act of 1934. The DTC settles payments related to its transactions through a connection to Fedwire.

2.1.4 Third-Party Processors and Other Services

Third-party processing companies are technology companies that have developed as a result of consolidation and the pursuit of operating efficiencies within the financial services industry. By contracting out all but core competencies, financial institutions can dramatically cut overhead, which has enabled the concentration of resources on critical business goals. Some institutions outsource entire departments and business processes, an increasingly appealing option to organizations that are under pressure to cut costs and increase profits. Technology-related outsourcing is particularly appealing because of the

[32] *The Depository Trust Company Annual Report*, 1996.

dynamic nature of the field. The high cost of leading-edge technology has driven many banks into establishing partnerships with third-party providers that can leverage their technology resources.[33]

Typical services offered by third-party processors include the following:

- Data center management
- Network management
- Application development, management and maintenance
- Check and statement processing
- Mutual fund account processing
- Electronic funds transfer
- Core technology implementation and support.[34]

Outsourcing has grown to the point that about 11 percent of the nation's 63 billion checks are now processed by a third party, excluding the Federal Reserve. About 68 percent of all credit card accounts are processed by nonbank third parties, and the largest processors of account transactions in the country are no longer banks.[35]

Currently, the top five financial services outsourcing firms by revenue in the United States are ALLTEL Information Services Inc, BISYS, Electronic Data Systems Corp., Fiserv Inc., and M&I Data Services.[36]

2.1.5 Regulatory Structure and Reporting Requirements

Federal and State agencies play an important role in regulating and supervising the activities of the financial services industry. The terms supervision and regulation are often used interchangeably with respect to the financial services industry, but they actually refer to distinct, but complementary, activities. Supervision involves the monitoring, inspecting, and examination of organizations to assess their condition and their compliance with relevant laws and regulations. When an institution is found to be noncompliant or to have other problems, the appropriate supervisory authority takes action to have the institution correct the problem. Regulation entails making and issuing specific regulations and guidelines governing the structure and conduct of financial services, under authority of legislation.

At the Federal level, supervisory and regulatory responsibilities are shared among the several authorities listed below.

- Federal Reserve Board
- Federal Deposit Insurance Corporation

---

33 Joanna Bers, "Outsourcing It All." *Bank Systems*, March 1996.

34 Ibid.

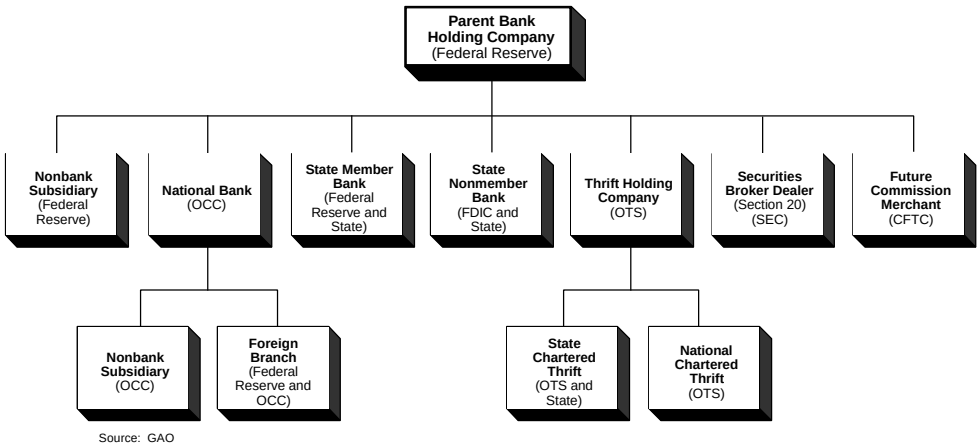
35 Diogo Teixeira, "Disaggregation: How Far Will It Go?" *American Banker*, July 31, 1996.

36 Joanna Bers, "The Future of Outsourcing," *Bank Systems and Technology*, August 1995.

- National Credit Union Administration (NCUA)
- Office of the Comptroller of the Currency
- Office of Thrift Supervision (OTS)
- Securities and Exchange Commission
- Commodities Futures Trading Commission (CFTC).

Figure 2-6 represents the regulation of a hypothetical bank holding company.

Figure 2-6. Regulation of a Hypothetical Bank Holding Company



Changing conditions in the financial services industry during the past several decades necessitated the closer coordination of regulatory and supervisory efforts. Consequently, the Federal Financial Institutions Examination Council (FFIEC) was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978. The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the FRB, FDIC, NCUA, OCC, and OTS and to make recommendations to promote uniformity in the supervision of financial institutions.

State governments also regulate and supervise the activities of banks chartered within their State. A number of international organizations, including the Bank for International Settlements and the International Organization of Securities Commissions (IOSCO), promote standards for regulation to maintain just, efficient, and sound markets. Figure 2-7 illustrates the Federal institutions with the responsibility for regulating and supervising banks.

Figure 2-7. Responsibility for Bank Regulation and Supervision

	Developing and Issuing Regulations	Licensing/Chartering Banks	Bank Information Reporting and Analysis	Bank Examinations	Enforcement Authority	Deposit Insurance	Failure Resolution	Lender of Last Resort	Crisis Management
Treasury[a]									●
OCC	●	●	●	●	●				●
OTS	●	●	●	●	●				●
Federal Reserve	●		●	●	●			●	●
FDIC[b]	●		●	●	●	●	●		●

[a] OCC and OTS Report To Treasury

[b] The Board of Directors of the FDIC includes the heads of OCC and OTS as well as three independent members, including the Chairman and the Vice-Chairman who are appointed by the President and confirmed by the Senate.

Source: GAO

The regulation and supervision of the markets and market participants is primarily the responsibility of the SEC, CFTC, and the SROs. The SEC is the independent, quasi-judicial regulatory agency with responsibility for administering the Federal securities laws. In general, these laws protect investors by ensuring the fair and equal disclosure of information concerning publicly traded securities. The laws also regulate firms engaged in the purchase or sale of securities, clearing organizations, people who provide investment advice, and investment companies.

In 1974, amendments to the Commodities Exchange Act (CEA) created the Commodities Futures Trading Commission to regulate the futures market. Before 1974, the Department of Agriculture was responsible for regulating the market. The CFTC has exclusive jurisdiction over futures and has established a comprehensive regulatory structure to protect the futures market and investors.

Also, the President's Working Group on Financial Markets was created following the October 1987 stock market crash to address issues concerning the competitiveness, integrity, and efficiency of the financial markets. The Secretary of the Treasury chairs the working group. Other members include the chairs of the CFTC, the Federal Reserve System, and the SEC.

3.0 RISK MANAGEMENT

The most striking characteristic of how the financial services industry protects its networks and information systems is the practice-consistent throughout all the institutions interviewed-of addressing information security and business continuity from an overall framework of risk management. Risk management is a continuous process of identifying, measuring, monitoring, and managing exposure to potential risks, regardless of their source.[37] The major

[37] Federal Deposit Insurance Corporation, Division of Supervision, "Electronic Banking: Safety and Soundness Examination Procedures," February 1997.

institutions at the heart of the industry manage hundreds of billions of dollars in assets against a global set of risks, which include extraordinary events such as war and international crises.

Access controls, system audits, use of diversely routed telecommunications circuits, disaster recovery plans, backup data centers, and all the many other information assurance measures were not viewed as independent efforts but as elements of an institutionwide approach to managing all types of risks. Fundamental principles of this approach are that no measure should ever be the sole control point in a transaction, and that no resource should ever be the sole means by which a function can be carried out. Much of the security and robustness of the nation's financial infrastructure is due to a consistent adherence to these principles across all sectors of the industry. For this reason, it is essential to describe the primary types of risks confronting financial institutions and the way in which information security and business continuity fit into an overall framework of risk management before discussing specific information assurance measures.

3.1 Definition of Risk

The *FFIEC Information Systems Examination Handbook* defines risk as the potential that events, either expected or unanticipated, may have an adverse impact on the institution's or firm's earnings or capital. As the handbook notes, "The existence of risk is not a reason for concern."[38] Indeed, at its core, the business of banks and securities firms is establishing trust and accepting and managing risks. The ability of an institution to understand and control risks is integral to its ability to make money and withstand adverse impacts. "Risk unto itself is not bad," one industry expert has commented. "What is bad is risk that is mispriced, mismanaged, misunderstood, or unintended."[39]

3.2 Types of Risks

No one risk management framework fits all financial services institutions. Different regulatory agencies, industry utilities, professional organizations, and individual institutions have defined different types of risks that must be considered. Virtually all these frameworks, however, identify the following as primary categories of risk:

- **Credit risk.** The risk of a customer, participant, or debtor failing to meet its obligations.

- **Compliance risk.** The loss to an institution that could result from violating or failing to comply with laws, rules, or regulations.

- **Market risk.** The risk to an institution's earnings or capital from changes in the value of its portfolio of investments due to actions in the markets in which it participates.

---

38 *FFIEC IS Examination Handbook*, 1996, page 2-1.

39 Leslie Rahl, Capital Markets Risk Advisors, in "CFTC's Interactive Symposium on Risk Management Practices and Internal Controls," Commodities and Futures Trading Commission, Washington, DC, March 1996.

- **Reputation risk.** The risk to an institution from a loss of public trust or confidence.

- **Transaction or operational risk.** The risk to an institution from an interruption, failure, fraud, or loss of its ability to provide services or deliver a product.

In addition, institutions using payments systems such as Fedwire, CHIPS, automated clearing houses, and credit-card associations deal with *systemic or settlement risk*: the risk that the inability or unwillingness to pay of one or more participants in a clearing and settlement system will cause other participants to fail to meet their own commitments.

3.3 Internal Risk Management Programs

Identifying the relevant aspects of each type of risk, measuring or assessing their magnitude, probability, and potential impacts, and establishing and enforcing appropriate controls are fundamental elements of a risk management program. Since risks are continually changing as the economic, regulatory, political, cultural, and technological environment changes, an effective program must include feedback and frequent reassessments to ensure these controls remain effective.

Risk management is not just a buzzword for financial institutions. The Office of the Comptroller of the Currency (OCC), for example, explicitly practices what it terms "supervision by risk" in national banks.[40] Supervision by risk focuses the attention and resources of examiners on those areas presenting higher risks to a bank. The OCC expects large national banks to have extensive formal risk assessment processes in place and working on an ongoing basis.

The banks interviewed for this study all identified the Federal Deposit Institution Corporation Improvement Act (FDICIA) as a strong motivator for their risk management programs. FDICIA requires the board of directors of large banks to report annually on the system of internal controls that ensure their safety and soundness and mandates stiff penalties for noncompliance. FDICIA and other regulations put bank directors in the position of having greater liability than directors in any other kind of company for losses incurred on their watch.[41] Even for nonbanks, risk management is viewed as an institutionwide concern. In its "Generally Accepted Risk Principles" for financial institutions, Coopers & Lybrand, one of the Big 6 accounting firms, puts it bluntly: "The ultimate responsibility for risk management must be with the board of directors. Risk management must be driven from the top down by those charged with overall responsibility for running the business."[42] Or, as Gary DeWaal, general counsel of

---

[40] Large national banks are defined as:
- A national bank with total assets of $1 billion or more, or
- A national bank that is part of a multibank holding company that includes at least one national bank with assets of $1 billion or more.

[41] Martin Mayer, op. cit, page 31.

[42] Coopers & Lybrand press release

FIMAT Futures, a major futures trading firm, has expressed it, "The doctrine of risk management really must be gospel for the entire congregation."[43]

Financial services is a business rooted in multiple, independent, and reinforcing checks and balances. Debits must equal credits. The practices of daily balancing and settlements have necessitated manual and automated systems to ensure transactions are regularly reconciled with outstanding items identified and resolved. These processes serve as basic risk management controls and help prevent fraudulent activity. When fraud or inaccurate transactions take place, these processes alert management and help in the timely resolution of problems.

This study found that in all major financial institutions—whether in banking or securities or futures markets—information security measures, practices, and policies were incorporated into an overall risk management process involving cross-functional reviews at several levels of management and ultimately reporting to the chief executive officer and board of directors. Although the details of the process varied from firm to firm, all included the following elements:

- Review of practices and policies by a committee or panel that includes managers from outside the information technology organization
- Mandatory review of all major changes, upgrades, or additions to applications, information systems, and networks
- Periodic reassessment of major systems, applications, and policies and reporting on results to this body
- Mandatory review of any waivers to existing policies
- Separation of duties and authorities so that personnel cannot initiate and implement major changes without independent review and authorization.

In addition to specific risk management programs, most institutions have implemented internal and external audit programs. These programs report independently to senior management or boards of directors on compliance with established risk management practices. The audits review both financial statements and operational activities. FDICIA requires that banks establish an independent audit committee composed entirely of independent outside directors—no customers are allowed to participate—to provide an unbiased review of its annual report and other activities.[44]

As part of the SEC's efforts to address the risks in the financial services industry, the Commission has in place a program that focuses on operational risks to market systems. The

---

43 In "CFTC's Interactive Symposium on Risk Management Practices and Internal Controls," Commodities and Futures Trading Commission, Washington, DC, March 1996.

44 Thomas Vartanian, David Ansell, and Robert Ledig, "FDICIA Has Important Implications for Bank and Thrift Board Rooms," *Banking Policy Report*, March 16, 1992.

SEC's Automation Review Policy recommends that self-regulatory organizations, such as exchanges, Nasdaq, and clearing agencies, conduct independent assessments aimed at identifying potential weak points in their systems and that the results of these reviews be presented to the SROs' senior management.[45] The Futures Industry Association also has recommended that exchanges and clearing houses be audited at least annually by an independent, external auditor, and that these institutions, in turn, should conduct periodic audits of their members.[46]

3.4 External Oversight and Regulation

Federal and State regulations have played a major role in the industry's adoption of the risk management approach. Even with increasing deregulation, financial institutions are still subject to close scrutiny and regulation. FDICIA, other United States Code (U.S.C.), and Code of Federal Regulations (CFR) provide standards for various aspects of the operations of financial institutions. The traditional safety and soundness examinations by the Federal and State banking authorities are augmented by information system examinations and supervision.

FDICIA and other regulatory changes have greatly expanded the purview of Federal examiners. The Federal Reserve, the OCC, and the FDIC have all increased their supervision and regulation staffs by 24 to 45 percent since 1988 to handle the increased workload. Information systems examiners account for a large share of these increases.[47]

A typical OCC bank examination can take up to a month for a mid-sized bank, and the largest banks are assigned a full-time team of examiners who work on-site. At the end of the examination process, which includes everything from checks on procedures down at the lowest level to interviews with the bank's senior managers, the examiners assign the bank a rating (known as CAMEL, for capital, assets, management, earnings, and liquidity). Banks strive for good CAMEL ratings, because top-rated institutions receive relief from the FDIC on paying deposit insurance premiums. Recently, the FFIEC added an "S" (for "Sensitivity to Market Risks") to the CAMEL system. To highlight the importance of an institution's risk management process, banks and bank holding companies are assigned a risk management evaluation as a significant part of the management ("M") element of their CAMEL rating.[48]

Although the SEC's Automation Review Program is considerably less extensive than that of FFIEC members, given the role of SROs, it does conduct a series of reviews annually and requires SROs to notify the SEC of any major changes to systems that might affect security or capacity to handle exceptional volumes. As part of its reviews, the SEC reviews the SROs'

---

45 Securities and Exchange Commission Release No. 34-29185, "Automated Systems of Self-Regulatory Organizations," File No. S7-12-91, 1991, and SEC Release No. 34-27445, 1989.

46 Futures Industry Association, "Financial Integrity Recommendations for Futures and Options Markets and Market Participants," June 1995.

47 General Accounting Office, "Challenges at the Federal Reserve Require Systemwide Attention," GAO/GGD-96-128.

48 Board of Governors of the Federal Reserve System, "Risk-focused Safety and Soundness Examinations and Inspections (SR 96-14)," May 24, 1996.

computer operations and facilities, telecommunications, systems development, capacity planning and testing, and contingency planning.

Backing up this oversight are sentencing guidelines for Federal courts that make it tough for defendants to get their sentences reduced in compliance cases unless they can prove that sound, documented practices were in place and that any infractions were isolated.

3.5 Threat Information and Risk Management

One question asked of the institutions interviewed was, "What could the Federal Government do to help you improve the security of your systems?" A common response was, "Provide more information on threats." As one bank security officer said, "Are there threats the government knows about that I don't know about? I need that information so I can manage those risks." Many of the institutions interviewed voiced the concern that they could not manage against cyber threats on the scale of "an electronic Pearl Harbor" because they had no credible evidence that these threats existed.

As discussed above, financial institutions manage against a wide range of risks, from fraud to bad loans to market changes to system outages. Given the global nature of business for many of these institutions, even wars and natural disasters are not uncommon events. Greed provides an eternal source of threats to a financial institution's assets. Institutions deal with potential for immediate and substantial financial losses on a daily basis, and as described in the next chapter, take all the steps that would be expected from a sound business perspective. The ability of an institution to maintain the trust, and hence, the business, of its customers is viewed as an even greater value than the dollars and cents involved. This suggests why many more layers of risk controls can be seen in the financial services industry than in perhaps any other infrastructure.

4.0 RISK CONTROLS

This study's focus was on those measures financial institutions had put in place to protect against risks to their networks and information systems. As described in Chapter 3, the study group found that most institutions dealt with these risks within the context of a comprehensive risk management process. It was not uncommon, this study observed, for information security issues to be addressed at the board of director level. This approach, as well as long experience in dealing with real-world threats, leads institutions to implement risk controls at several levels. This chapter describes the risk control measures observed among the institutions interviewed, including those related to:

- Policy and organization
- Personnel
- Information systems
- Telecommunications
- Disaster recovery.

4.1 Policy Risk Controls

Within the industry, risk management is manifested in formal, comprehensive, and regularly reviewed information security and disaster recovery policies. In some cases, they are mandated by regulations such as FDICIA or recommended by guidance, such as OCC circulars and Federal Reserve Supervisory letters. Even in such cases, they are also driven by business needs for the availability, reliability, and security of networks and information.

Starting at the basic level, institutions typically had a guide to information security responsibilities that was included in all new employee packages. Formal training on security was a part of mandatory orientation sessions. All employees were instructed in their basic responsibilities, such as protecting passwords, not disclosing information about the institution's systems, and reporting unusual activity. A number of institutions prepared security orientation video tapes that were introduced by the chief executive officer to reinforce the understanding that this was a priority concern at the highest level.

Not all institutions, however, had guidelines in place for the protection of information itself, regardless of the format or system involved. Although information was commonly marked as "proprietary," it was not clear that the rules for determining if a document or piece of information was proprietary were standardized, widely communicated, or consistently applied.

Ensuring customer information privacy adds to the information control challenges. Firms doing business internationally pointed out that, in some countries, laws regarding the confidentiality of personal information forced them to adopt very strict security measures. One firm reported that it was engaged in a corporatewide review, whose goal was to establish a four-tier information classification system and begin implementing the system throughout its manual and automated processes.

A principal element of an effective information security program is formally assigning responsibility and accountability within the organization. In every institution interviewed, the job of managing information security was assigned to a particular individual; and in every major institution, this was a full-time position no more than two levels down from the board of directors. In many cases, information security was combined with disaster recovery responsibilities under one manager. Physical security, however, was still managed by a separate group.

The number of full-time information security staff ranged from several people to more than 200, based primarily on whether the institution took a centralized or distributed approach. Large staffs were employed in institutions where administrative tasks such as assigning passwords and creating or deleting accounts, were handled by a centralized information security office. A much smaller staff was seen when these tasks were delegated to information systems or business unit personnel.

Several institutions combined a dedicated information security function with an advisory council, with representatives drawn from business units throughout the organization. These councils reviewed and recommended changes to systems, policies, and procedures, and the representatives often served as additional focal points for security within the individual business units.

The information security function appeared to be vested with authority commensurate with its responsibilities. Waivers to established security policies and systems generally required review by the information security office and authorization at a very senior level. The manager signing off on a waiver usually had to assume responsibility for any resulting risks. Several firms interviewed described their waiver process and then commented that they could not recall any waiver ever being approved.

Information security was also considered to be an integral element at the onset of major system changes or technology investments. Many institutions have an investment committee or council that regularly brings together senior business and technology executives from different business units. It was not uncommon for information security personnel to have significant input into new product and distribution channel development.

As a result, information security and other policy risk controls are accounted for during the development of business operations rather than as an afterthought. This approach also provides a greater appreciation of information security concerns across all sectors of a particular institution. One information security officer interviewed credited his corporate investment council for the level of information security within the institution. Several managers recalled instances when the deployment of a new service or system was halted as a result of the risks identified during this kind of investment review.

The extensive internal audit function within financial institutions also helps to reinforce the work of the information security staff. The internal audit staff for most of the major institutions includes certified data processing auditors and reports to a separate management chain from that of information security or the information systems operators.

Many of the interviews highlighted concerns about enforcing security policies in outsourcing or partnering arrangements. Although some firms included clauses requiring contractors to follow practices equivalent to their own, managers acknowledged that they were unsure whether these conditions were enforceable because the whole question of what constitutes "best practice" in information security is just beginning to be addressed.

4.2 Personnel Risk Controls

The risks associated with personnel are a significant concern for financial institutions. The industry is extremely cognizant of the fact that the people with the most detailed knowledge and access to financial networks and systems pose the greatest threat to any institution. The financial services industry practices extensive personnel risk controls, starting with the interview process and continuing through termination of employment.

In general, the institutions interviewed had strict screening processes for prospective employees. All institutions conducted background investigations that included State and national agency checks, and many institutions conducted drug testing either as a prerequisite to hiring or on a random basis among all employees. The study group observed that the industry tended to

avoid hiring individuals with anything more than minor misdemeanor convictions, and enforced those standards after employment. One institution had a zero tolerance policy towards dishonesty-based crimes, and fired employees for infractions such as stealing a plant from the office or jumping a subway turnstile. Institutions were also intolerant of any falsification of educational credentials, job history, or references on employment applications.

All of the institutions interviewed expressed the frustration that fear of liability has led most companies to limit the information they release on former employees, often providing nothing more than their dates of employment. Although an institution might be scrupulous in terminating employees for misconduct or misrepresentation, it is leery of its potential liability if negative information is released to future employers.

The length of time it takes to complete background checks, particularly for national level checks, which average 4 to 6 weeks, also raises significant concern for financial institutions. Few firms isolate or restrict new employees who have pending background checks. Several institutions reported that they had hired employees who had to be terminated when their background checks revealed unfavorable information.

In addition, personnel security among contract staff was a recurring concern. Where the function was outsourced and performed wholly within the contractor's own facility, this risk was minimized by limiting interfaces to the institution's own systems and by requiring equivalent standards for background checks or bonding as an alternative. There was less assurance, however, about consultants and contractors who work in an institution's own facilities alongside its own staff. Because these arrangements can be made at a low level within a business unit, screening standards are enforced less consistently throughout an institution.

Many institutions voiced misgivings about the potential exposure of system information because of extensive reliance on outside programmers to develop and test solutions to Year 2000 software problems. The senior information security officer of one institution stated that his biggest fear was the possibility of malicious software code being introduced by the subcontractors working on this problem.

The institutions interviewed, on the whole, deleted user IDs and passwords and collected badges and other employee identification upon termination. In some instances, network access was revoked before the employee received termination notification. However, those institutions that did not maintain a centralized database of system accesses stated that it was possible their termination procedures might not include all systems to which an employee had access.

4.3 Information Systems Risk Controls

The financial services industry has evolved to a point where it would be impossible to operate without the efficiencies of information technology and networks. As Martin Mayer

observed, "Everything that happens gets entered into the computer about instantly."[49] Consequently, information systems risk controls are paramount to financial services institutions.

The applications, systems, and networks used by the major financial institutions are extraordinarily complicated. This complexity may represent the single greatest security risk because the array of mainframes, midframes, desktop clients, operating systems, databases, middleware, messaging, network transports and protocols, gateways, remote accesses, and network interfaces operated by a typical institution far outpaces the ability of management tools to track them. However, this heterogeneity also helps reduce the risk of the system being undermined by a single vulnerability.

Information systems risk controls implemented on a widespread basis throughout the financial services industry include the following:

- Access controls
- Applications controls
- Procedural controls
- Fraud controls
- Data network controls
- Encryption.

An essential point to emphasize is that none of the institutions interviewed relied on any one control measure to ensure the authenticity, confidentiality, or authority of a transaction. This multilayered approach to security, in fact, is one of the industry's core strengths.

4.3.1 Access Controls

Major financial institutions have relied on mainframes for core applications processing since the 1960s. Even 30 years later, mainframes and fault-tolerant midframes operate the most critical applications. Institutions benefit from the maturity of mainframe technology in many ways, including access control, system management, and backup and disaster recovery.

Those operating mainframes rely on Resource Access Control Facility (RACF) and similar applications to manage user accounts, passwords, and access privileges centrally. Mainframe controls, combined with connection-oriented protocols, such as bisynch and IBM's Systems Network Architecture (SNA), provide an easy way for institutions to maintain effective access controls with centralized management and auditing with a high degree of nonrepudiation. In contrast, the ability to spoof network address information in transmission control protocol/Internet protocol (TCP/IP) was cited as a major reason institutions were reluctant to move away from mainframe-era protocols, despite the other technical and cost advantages. Nevertheless, the shift to TCP/IP is considered inevitable for economic and interoperability reasons.

[49] Mayer, op.cit, p. 19.

Although approaches differed among institutions, password management practices were more rigorous than those in other industries. Many institutions enforced standards that make passwords difficult to guess or crack, but even those that did not compensated by mandating frequent changes—as often as once a month. Wherever a tool to do so was available, passwords were aged and users forced to select new ones periodically, usually every 3 to 4 months.

Several institutions also established profiles that matched system and application accesses against typical jobs. In some cases, these profiles were provided to business unit managers as guidelines to use in approving new access requests. In one case, the information security function generated a monthly report that flagged users whose access exceeded their respective profiles and required managers to review and acknowledge it.

Most institutions were interested in moving to a single sign-on approach so that a single user ID and password could allow a user to access all required information resources. However, most institutions felt that the commercial products offering this capability were not ready to be deployed because they were too immature or difficult to manage.

A few institutions prohibited any remote access to their core operational systems. Others allowed remote access only in exceptional situations, for backup or emergency maintenance, and controlled it by initiating any calls from their facility and monitoring activity during connections. In most cases, remote access was used extensively, whether for telecommuting, customer services such as wire transfers and cash management, or for remote administration and maintenance by staff or vendors. Most institutions interviewed had installed a token-based access control system to supplement existing access controls.

4.3.2 Applications Controls

Accessing an institution's information systems does not, however, necessarily open up a treasure chest. It's not uncommon for user interfaces and commands for the most sensitive applications, such as wire transfer, to be designed intentionally to prevent all but trained and authorized operators from executing transactions. Some institutions even created "honey pot" applications to divert possible intruders from the legitimate application.

Wire transfer is often cited as the most vulnerable of all financial institution applications. It is one of only a few core applications that are interactive and also involve potentially large sums of money. Generally, institutions tend to trade off interactivity and transaction value. Applications involving on-line interaction from a customer, such as withdrawing cash from an ATM, do not usually involve large values. Interbank payment messages to CHIPS or Fedwire, on the other hand, which can involve billions of dollars, are handled via highly structured messages, not interactive commands from a user. Both Fedwire and CHIPS employ encryption at one or more layers to authenticate messages and secure connections to customers.

For reasons of operational reliability as much as security, most institutions carefully isolate support staff from operational systems. The most critical operational systems are stripped of all nonessential elements, including editors, compilers, and other tools that might be used in an

information system attack. Software development staff are prohibited from accessing operational systems, and the transfer of updates from development generally goes through a rigorous review and approval process that includes a requirement for having a reliable way to back out of any update.

Viruses are not a significant threat to core financial applications, but major institutions rely on networks of hundreds, thousands, and even tens of thousands of personal computers for administrative and support functions. Virus screening programs and tools are in place at all the institutions interviewed, but many reported that viruses still cause the majority of their information security incidents. However, the damage resulting from viruses-aside from productivity losses-was judged to be negligible.

4.3.3 Procedural Controls

Financial institutions are heavily dependent on information systems, but they tend to be skeptical about trusting an information system's security. For this reason, numerous procedural controls are overlaid on the various information security controls. Many of these controls are derived from procedures that were in place before automation.

Many core financial applications are proprietary or extremely customized vendor software products. This makes them resistant to traditional cyber type attacks and reduces systemic risks. Other institutions believe that commercial products may be more secure because of wider public examination.

At major institutions, business units employ distributed client/server-based applications, both commercial off-the-shelf (COTS) and proprietary. Other financial institutions generally, and smaller banks especially, may use vendor developed platforms and applications with very little customization. Many of the custom applications that banks have deployed in the mainframe environment have little or no on-line documentation and are user unfriendly or even cryptic, thus making attacking them time and labor intensive.

The segregation of duties between operational and development staff described previously is one example of a procedural control. Another occurs in wire transfer applications. Because of the large risks involved, many of these systems require third- or even fourth-party confirmation. A request for a transfer cannot, by itself, generate the transfer. Instead, the request will be confirmed through a telephone call back to a different person at the originating institution. Authentication codes or challenge-response codes may be used as an additional check. Some systems will require this additional confirmation for all requests; others will screen requests and route a few for confirmation follow-up, based on a random sampling or preset detection filters.

In the securities and commodities business, clearing and settlement of trades generally involves an even stronger procedural control: no trade is executed unless both parties affirm it, along with all necessary details, to the clearinghouse. Every buy must be matched with a sell. Mismatched trades will be kicked back to the brokers for resolution; unmatched trades can be rejected out of hand. Trading automation has actually improved the security of transactions by

providing exact time-stamping of trades, something that could be fabricated in the days of open-outcry.[50]

4.3.4 Fraud Controls

Some procedural controls can serve to prevent or detect fraudulent activities by inside staff. Most financial information systems include other measures designed to detect fraudulent transactions, regardless of the source. Much of fraud control relies on the experience of financial institution officers and the promotion of a culture of risk management.

The majority of fraud controls are established within defined systems. Examples include sophisticated pattern recognition software designed to detect check kiting (account balance manipulation) or account profiles that highlight transactions that fall outside normal customer activity. Some fraud controls are established at an institutionwide level. Credit and exposure limits and experience data available through institutionwide customer information systems assist in risk management efforts.

Examples of systemic fraud controls include the shared card application fraud system jointly operated by Visa and MasterCard. A new type of fraud control system has emerged: Card Alert Services, a multibank and network owned company, works with bank card issuers and ATM/point-of-sale (POS) networks to detect and contain systemic card fraud. The organization collects information on unauthorized transactions. In addition, proprietary processes identify the source of the compromise and tell issuers what cards could have been compromised. Issuers and networks then block those numbers and issue new cards to contain the fraud. The effect is improved resistance to low-level fraud and catastrophic compromise.

4.3.5 Data Network Controls

Through the early 1980s, most data networks were built on proprietary protocols, usually bisynchronous, and centered on one or more mainframe data centers. This is still the structure of many financial networks. In some cases, fault-tolerant midframes, mainly from Tandem, have been added to, or have replaced, the mainframes; and SNA and X.25 have replaced bisynch. But concerns about security, reliability, and manageability have kept many institutions from updating their network model.

This architecture does not mean that financial institutions have not adopted newer and more open network technologies. In fact, the number of network access points or possible points of compromise have risen by orders of magnitude as the number of branches, services, and other operations have grown, and as telecommuting has become institutionalized. As the number of access points has multiplied, control over the means by which customers access remote delivery channels has declined. Clients are increasingly specifying their choices of equipment and software, and demanding that institutions accommodate their desires.

---

[50] *New York Times*, February 13, 1989, quoted in Carole Brown, "Control of Computer-Based Information System," http://www.bus.orst.edu/faculty/brownc/lectures/controls/control2.htm, January 25, 1995.

The growing use of client/server technologies has further complicated the work of information security officers. There are fewer security products available for client /server systems, and exercising control over applications and equipment is more difficult than in a monolithic mainframe environment. Maintaining current backups of data and applications is also far more difficult in a distributed environment. Re-establishing operations and recovering on a distributed network after a disruption form an arduous task that requires a significant degree of intelligent cooperation between information technology specialists and the business units.

TCP/IP protocols and networks are more open, and security tools less mature, than those of mainframes. There is a clear cost advantage to building on TCP/IP versus X.25 or SNA, however. Where the cost and technical advantages clearly outweigh the security risks, institutions are quickly integrating TCP/IP into their internal networks and for inter-institution networking.

Use of TCP/IP does not necessarily imply Internet use. In several cases, private TCP/IP networks are being established among institutions concerned that the Internet itself cannot provide an adequate level of reliability or sufficient end-to-end response times.

Banking and other financial uses of the Internet have received a great deal of attention recently. Most institutions view the Internet as a very high-risk environment, and isolate their web sites from all internal systems. Sites that allow customers to access account information and initiate transactions are not directly linked to the actual cash management systems holding their funds. Data is exchanged between the two systems once or twice a day, usually manually, through batch file transfers. This approach is similar to that taken for home PC and telephone banking systems.

Remote access authentication systems are currently used on a limited basis within an institution's internal information security perimeter. Retail delivery mechanisms, such as home banking, may incorporate a variety of authentication schemes including passwords, personal identification numbers (PINs), use of automated number identification, or dongles (outboard hardware devices). Personal Computer Memory Card International Association (PCMCIA) cards, smartcards, software implementations of challenge response systems, or digital signature systems are being piloted and may become commonplace as implementation costs fall.

No institution interviewed by the study group cited any theft due solely to an external electronic intrusion. Every instance of computer crime discussed in the study group's interviews involved insider collusion or circumvention of internal risk controls by employees or outside consultants.

Several institutions interviewed by the study group regularly perform penetration tests of their security systems, using staff or hiring consultants to perform the evaluations. At the same time, however, many institutions expressed interest in and frustration with intrusion detection tools. One institution stated it failed to meet a goal it had set of deploying a quasi-realtime intrusion detection mechanism in 1996 because it did not find a satisfactory product on the market.

4.3.6 Encryption

Encryption is the process of scrambling data according to a mathematical algorithm. By scrambling the data, its confidentiality is maintained. There are two basic types of encryption: symmetrical or secret key and public key /private key. Symmetrical encryption requires all parties to know the same secret key and is represented in encryption standards such as Data Encryption Standard (DES). Public key/private key encryption provides two keys. The first key is the public key, known by anybody. The second key is the private key, known only to the owner. Encryption with a public key allows only the holder of the private key to decrypt the message. Encryption with the private key facilitates proof of authenticity and message integrity through decryption with the public key.

Public key encryption standards are still emerging, resulting in incompatibilities between competing vendors. Standardization of the public key infrastructure needs to be established before a standard suite of encryption tools becomes available for all applications.

Financial institutions are among the most active users of encryption in industry. The DES, released in 1977, is the primary method used by financial institutions to encrypt sensitive information. Institutions primarily use encryption for authentication, secure data transmission, and protection of sensitive information such as PINs. Most encryption systems used in the financial services industry rely on hardware-based encryption. PIN protection systems typically employ dedicated encryption processors that also store the PIN data so that unencrypted PINs are not transmitted over any part of the network.

The Federal Government has long recognized the need for extra security in financial networks, and export controls on encryption products have traditionally included special exceptions for systems to be used in financial communications. All the institutions interviewed that operate international networks deploy bulk encryption on links outside the United States, in recognition of the increased threat of eavesdropping and monitoring overseas.

Because DES is mature, a transition process to an Advanced Encryption Standard (AES) has been initiated by the National Institute for Standards and Technology and the American National Standards Institute X9, the financial services industry standards organization. Public key technologies used by financial institutions or under development for that environment include RSA and elliptic curve algorithms. The Federal Government has also developed a secure hash algorithm and standard, a digital signature standard, and several secret cryptographic algorithms with a myriad of applications.

As home financial services are offered, many consumers and commercial customers will rely on off-the-shelf vendor provided browsers for encryption services to ensure transaction confidentiality and integrity. A majority of users of current browser enabled encryption are using a 40 bit key, which is considered inadequate by many financial service institutions. It is essential that larger encryption keys be offered and used by consumers to maintain transaction integrity and confidentiality.

Financial services institutions are considering extending the encryption of transactions to include more robust authentication through the use of digital signatures. Indeed, these institutions are among the leading candidates to serve as Certificate Authorities, which issue and manage digital certificates to authenticate public keys in any of their applications.

As more consumers use electronic access channels, the requirement for secure communications becomes paramount and global in scope. These consumer requirements may increasingly conflict with export restrictions on encryption technologies.

4.4 Telecommunications Risk Controls

The financial services industry is critically dependent on telecommunications networks. The availability and reliability of telecommunications services was a concern voiced by every institution interviewed by the task force. Increasingly, financial institutions are investing heavily in leading-edge telecommunications technologies, such as frame relay, integrated services digital network (ISDN), and asynchronous transfer mode (ATM) to transport ever increasing streams of data, voice, and video at high speeds. In a few cases, the study even found that institutions had installed private fiber optic lines to provide data communications at rates above those of any currently tariffed service. Financial institutions also invest heavily in means to ensure network availability. In 1996, it was estimated that banks alone spent about $4.1 billion on telecommunications services, placing the industry among the top consumers of communications systems and services.[51]

To mitigate the risk of business interruptions stemming from telecommunications network outages, financial services institutions have actively pursued telecommunications diversity by contracting with multiple providers of both local exchange and long-distance services. In the New York metropolitan area, financial services institutions rely on NYNEX as well as Metropolitan Fiber Systems (MFS) or several other competitive access providers for their local exchange services. In other areas, however, alternative local access is not yet available.

Unfortunate experiences and lessons learned from competitors have driven the adoption of network diversity. A fire in NYNEX's Broad Street central office led Wall Street firms that had not already done so to establish connections to an alternate central office. In 1993, as a result of its work in responding to the World Trade Center bombing, NYNEX began offering several network recovery services to improve the process of establishing communications to backup sites or to deal with the loss of a servicing central office. Over half of the customers using these services exercise them at least annually.

Fiber optic cable cuts are the most common cause of disruptions and every institution interviewed tended to divide its long distance circuits among multiple carriers and request diverse

51 "Telecommunications Spending Balloons As Banks Upgrade Systems and Services," *American Banker*, October 16, 1996.

routing.[52] As many have found, diversity is an elusive target. Different long-distance carriers may ultimately share the same facility or cable or resell network bandwidth to each other. Limitations in local access or physical facilities can undermine measures assumed to provide diversity.

Most of the financial service companies interviewed provide separate and distinct local exchange carrier access to their facilities. Often, the access is at opposite sides of the building. Within the building, diverse risers for routing telecommunications lines are used. Several institutions had microwave links established for back up communications. Notwithstanding these redundant arrangements with telecommunications providers, many respondents have also subscribed to tariffed services, such as synchronous optical network (SONET), to provide realtime reconfigurable network solutions to local exchange interruptions.

Clearly, the availability of diverse routing between the institution's premises and the local exchange office remains the primary chokepoint. In major metropolitan areas where alternate access carriers have installed their own network infrastructures, the study found institutions taking advantage of competition to improve their diversity. However, even competition in the local loop cannot guarantee diversity. Local exchange carriers share right-of-way to many buildings because only one route is available. Despite assurances about diverse networks from the carriers, a consistent concern among the financial services industry was the trustworthiness of their telecommunications diversity arrangements.

Under Telecommunications Service Priority (TSP) System, a program mandated by the Federal Communications Commission (FCC), telecommunications carriers are required to provide priority restoration of service to certain qualified users. The Federal Reserve has been designated as the sponsoring agency for requests for TSP use by depository institutions. The Federal Reserve has adopted criteria providing TSP sponsorship for backbone circuits of eligible private sector interbank large value-funds or securities transfer systems and access circuits that connect participants to a sponsored large-value payments system.[53] The NYCHA and SWIFT currently take advantage of Federal Reserve-sponsored TSP.

Intense competitive pressures are driving financial institutions to develop alternative means (e.g., Internet banking) for customers to access traditional financial services. Increasingly, these new alternative delivery channels are using the public network to reach customers. This issue is discussed in detail in Chapter 5, Industry Trends. Relative to this chapter, the primarily observation is that the increased use of public networks is a considerable and recognized source of risk for the financial institutions interviewed by the task force.

4.5 Disaster Recovery Risk Controls

Financial institutions view disaster recovery as an aspect of transaction or operational risk-the risk to the institution from any failure in its ability to provide services. The study group found

[52] Network Reliability and Interoperability Council report [ref].

[53] Federal Reserve Board Notice, "Telecommunications Service Priority," Docket No. R-0786.

that the leading firms and the infrastructure's major utilities have made significant investments to ensure they can respond to a wide range of contingencies with minimal interruptions in service to their customers—as well as minimal effect on their capital and shareholder equity.

There are strong business motivations for financial institutions to have sufficient resources and effective plans for coping with natural and man-made disasters. With the velocity of current financial systems, even short-term outages can result in major financial losses for a firm. In addition, the industry has dealt with a variety of crises over the last decade that have given it numerous opportunities to test and refine its disaster recovery capabilities. In fact, a number of firms interviewed are now working towards a goal of continuous operation, in which critical functions can be performed in any contingency short of the complete destruction of all systems and facilities.

Banks, securities firms, and industry utilities approach disaster recovery slightly differently. Banks tend to operate on a basis of settling their accounts at the end of a business day, which means short outages during the course of a day may not have significant effects if the bank has enough time left during off-hours to complete its settlement processes. On the other hand, Federal regulators expect banks to maintain disaster recovery plans, and bank examiners review these plans in detail. The Office of the Comptroller of the Currency's Bank Circular 177 holds bank boards of directors responsible for having a thorough and effective disaster recovery process.

Securities firms operate in the dynamic environment in which the value of assets changes constantly as trades are being negotiated and transacted through exchanges and over-the-counter deals. In this environment, a firm's bottom line can fluctuate dramatically in a matter of minutes. One disaster recovery consultant estimated that a typical securities firm's losses from a one-day outage could exceed $25 million.[54] Fierce competition provides a strong incentive for firms to stay on-line. As the information protection manager of a leading brokerage commented during an interview, "It's OK if everyone in the market goes down. The worst scenario is to be the only one who goes down."

The key industry utilities, whether they support banking or securities and commodities, are all characterized by a tremendous daily volume of transactions. The Options Clearing Corporation, which handles the clearing activities of options exchanges, processes nearly one million transactions a day. The CHIPS and Fedwire routinely receive 5 to 10 funds transfer messages each second during peak traffic periods. One credit card association estimates it processes more than 2,000 authorization requests per second during the Christmas holiday shopping rush and expects to be handling 5,000 requests per second by the year 2000.

Dealing with this kind of volume, industry utilities cannot afford any interruption in service. Most of these utilities are funded through the transaction fees paid by their customers, and a loss of service has a direct monetary effect. System outages create huge backlogs that could quickly exceed the utility's resources to catch up. Utilities have developed highly

---

[54] Ivy Schmerken, "Spending on Trading Recovery," *Wall Street and Technology*, April 1994.

optimized, carefully managed systems to handle their transaction workloads, including sophisticated, well-tested procedures for distributing the load and switching between systems—whether on-site or to another data center—in seconds or, at most, a few minutes.

Regardless of their motivations, the leading financial institutions take a multilayered approach to building robustness and recoverability into their systems. Operational data centers are engineered from the ground up with survivability in mind. Some are hardened with thick concrete walls and protected with extensive perimeter security measures equivalent to military command posts. Most have uninterruptible power supplies, generators, and on-site fuel storage sufficient to allow the facility to run independently of the power grid for a period ranging from a few hours to over a month. External telecommunications links are diversely homed, with multiple building access points and connections to more than one central office or point of presence wherever possible. Operational procedures within the data center are designed to minimize the risk of human errors causing interruptions, and most or all data files are copied and stored on disk or tape at off-site facilities.

Few of the major institutions rely on a single data center. Most have at least a primary and a backup facility, often with both on-line and running in parallel. In a few cases, there is even a secondary backup facility. Those without a secondary backup have contracts and arrangements in place with computer system disaster recovery firms such as Comdisco, IBM, or Sunguard. However, when it comes to backups, it is possible to have too much of a good thing. As the Federal Reserve Board concluded when it chose to consolidate essential processing from 12 data centers down to 3, there is a point at which the reliability problems introduced from having to manage system configurations and procedures at multiple facilities outweigh the potential benefits from diversity.

The introduction of client-server and PC systems has greatly complicated disaster recovery challenges. The maturity of backup and recovery technology for mainframes has been key to the speed and effectiveness of these backup arrangements. The tools for balancing loads, switching processing functions, and recovering files from memory and disk between mainframe systems have been developed and refined over the last 2 decades. This longevity is part of the reason most of the major institutions interviewed expect to keep their critical transaction processing applications on mainframes for the foreseeable future. One bank interviewed reported that the first time it attempted to recover a client-server application to a backup site, it took over 24 hours to properly configure the system and restore all the necessary files.

The proliferation of smaller systems outside the core data centers has also added to the problem of keeping track of what is critical to business functions from the standpoint of backup and recovery. Numerous firms have found that their disaster recovery arrangements did not cover one or more systems that had evolved from nonessential prototypes into vital business tools.

Numerous natural and man-made disasters over the last decade have forced financial institutions to test and refine their disaster recovery capabilities. Firms in California have dealt with major earthquakes in 1989 and 1994, as well as civil disturbances in the Los Angeles area following the Rodney King beating trial in 1992. A rainstorm in late 1992 flooded electrical

vaults and forced several major Wall Street firms to shift to their backup sites.[55] A blizzard in 1993 caused the roof to collapse on the EDS data center in New Jersey handling thousands of ATM terminals; and EDS had to locate, equip, and recover operations to a new data center in a matter of days. Institutions in the Southeast have dealt with evacuations and destruction from Hurricanes Hugo and Andrew.

The industry's dependence on other infrastructures has been tested by a series of recent disasters. In 1988, a fire in the Ameritech central office in Hinsdale, Illinois, knocked out long-distance telecommunications for the Chicago Board of Trade and other major institutions. An electrical fire in a Consolidated Edison office in August 1990 blacked out one side of Wall Street for nearly a week. Underground flooding in downtown Chicago in April 1992 caused sustained telecommunications and power outages. And institutions in the West had to deal with widespread electrical power outages during the summer of 1996.

The industry has also dealt with man-made disasters, including the 1993 terrorist bombing of the World Trade Center. These real-world experiences have forced institutions to deal with deficiencies and unexpected problems that would never be encountered through exercises alone, and have provided significant additional motivation for investments in physical security and disaster recovery. One firm interviewed reported that its board approved over $12 million in additional backup and recovery measures following the World Trade Center bombing and another said it initiated an $8 million program to secure the perimeter of its data centers following the Oklahoma City bombing in 1995.

Each of these incidents ultimately led to improved robustness of the financial services infrastructure because it not only forced the institutions affected to overcome recovery problems but tended to spur other institutions to examine their own capabilities. As a result, this study found that the financial services institutions not only had made considerable investments to minimize the risk of outages affecting their ability to deliver essential services, but had gained substantial experience in dealing with a range of contingencies, including outages affecting other infrastructures.

5.0 INDUSTRY TRENDS

The financial services industry is undergoing several fundamental changes that are reshaping the industry landscape. The key drivers transforming the industry are fierce competition between and within all sectors of the industry, consolidation, deregulation, and emerging services and technologies.

5.1 Banking Trends

Traditionally, commercial banks have provided three basic functions for consumers and institutions-deposits, loans, and investment opportunities. Now, banks are experiencing competition on all three fronts by competitors such as credit card companies, mortgage

[55] Ivy Schmerken, op. cit.

companies, government-sponsored enterprises (e.g., Freddie Mac), specialty automobile finance companies, specialty home equity lenders, and brokerage and mutual fund companies. Consequently, the banking industry has experienced a significant decline in its control of U.S. financial assets. In 1950, commercial banks alone held 42 percent of all U.S. financial assets; by 1980, that figure was down to 38 percent. In 1995, it had plunged to 9.1 percent.[56]

Although the banking industry's share of the total U.S. financial assets may be declining, there is a significant and increasing concentration of financial assets among large banks. Banks with more than $1 billion in assets increased their share of industry assets to almost 75 percent in 1993, up from just over 60 percent in 1980.[57] Within the last several years, there has been a tremendous amount of merger activity, marking the early stages of a landmark consolidation process. In the 1990s, the number of banks has fallen from 14,000 to about 10,200 (see figure 5-1). Many industry experts believe there will be at least one-third fewer banks in a few years. During the first three quarters of 1995, bankers announced 389 mergers valued at $57 billion, more than double the previous record set in 1991.[58]

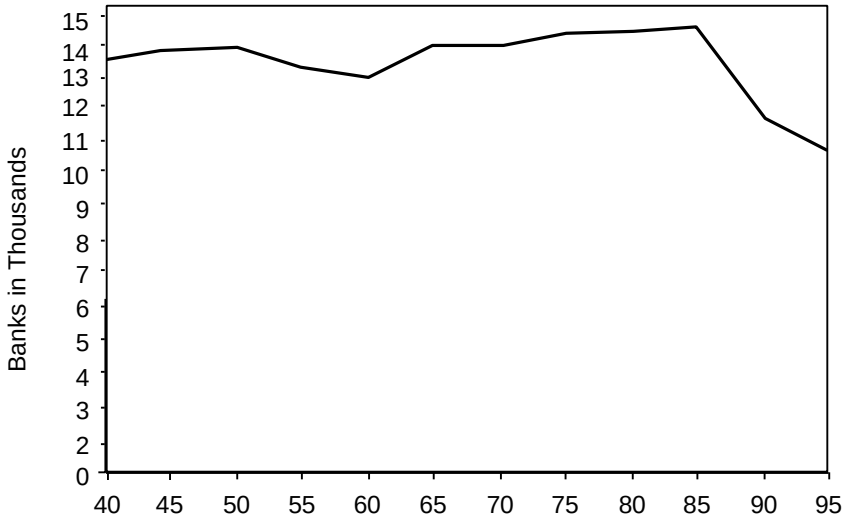
The consolidation that is occurring this decade represents types of mergers driven by compelling economic reasons. One is the merger among local competitors designed to cut costs, improve efficiency, and expand market share. The other is the amalgamation of banks in adjacent regions designed to create an institution that operates over a geographically large area while concurrently achieving economies of scale. The merger between Chemical Bank and Chase Manhattan Bank, announced in 1995, which created the largest single bank in the United States, is the preeminent example of a merger of two local competitors.

Figure 5-1. Number of Banks in the United States, 1940 through 1995

56 "Statistical Information on the Financial Services Industry," American Bankers Association, Seventh Edition, 1996.

57 Daniel Nolle, "Banking Industry Consolidation: Past Changes and Implications for the Future," Office of the Comptroller of the Currency, April 1995.

58 Serge Bellanger, "Choose Your Partners: The Era of Banking Consolidation," *Bankers Magazine*, March/April 1996, Vol. 179, p. 19-23.



Note: "Banks" Are FDIC-insured Commercial Banks and Trust Companies at Year-End.

Source: Office of the Comptroller of the Currency

However, many of the most significant acquisitions are those involving banks in adjoining regions. Examples include First Chicago joining with NBD and PNC of Pennsylvania with Midatlantic of New Jersey. Moreover, NationsBank, BancOne, and Key Bank have each expanded through a series of mergers with banks in other regions. Some banks have pursued both types of mergers: Bank of America not only merged with its California rival, Security Pacific, but also made acquisitions in several western states and as far east as Illinois.

Deregulation is also hastening the consolidation trend. For decades, U.S. banking was prohibited from consolidation by a regulatory framework that artificially maintained the decentralized structure of banking. The strict geographic limits on banking are now changing, permitting the consolidation process to proceed. In addition to interbank consolidation, many bank holding companies are consolidating within their organizational structure. The intense competitive environment has also compelled banks to seek relief from Depression-era legislative and regulatory restrictions limiting the markets in which these institutions are allowed to compete.

Proposals for diversification of the financial services industry would amend laws limiting affiliations and activities of banking organizations. Chief among these are the Glass-Steagall Act, which separates banking and securities business, and the Bank Holding Company Act, which regulates companies controlling banks. Such laws have the reciprocal effect of preventing other forms of enterprise from owning banking organizations or offering banking services.

The Congress has not recently passed any landmark legislation restructuring the financial services industry. The commingling of depository services with other forms of financial and/or commercial enterprise remains a subject of debate by legislators and regulators.

Notwithstanding the legislative inaction, many forces are changing the environment in which financial institutions traditionally have operated and individual types of institutions have competed. Technological advances, marketplace innovations, regulatory interpretations, and court decisions are all contributing to lessening distinctions among banking and nonbanking institutions.

For example, in 1996, the Federal Reserve increased from 10 to 25 percent the amount of total revenue that a nonbank subsidiary of a bank holding company may derive from underwriting and dealing in securities.[59] And on January 9, 1997, the Federal Reserve requested comments on the issue of removing a majority of the prudential limitations that currently apply to bank holding companies engaged in securities underwriting and dealing.

As these current service restrictions are relaxed, banks are in position to be the dominant acquirer of other financial services industry providers. The nation's 25 largest banking companies have $458 billion of market capitalization.[60] This market capitalization is significantly larger than those of the 25 largest companies that banks would most likely acquire in other sectors. The merger of Bankers Trust and Alex. Brown & Sons Inc. are likely harbingers of the type of cross sector partnerships the financial services industry will witness in the next 5 years. Ultimately, as consolidation continues, the financial services market could be dominated by a small group of well-capitalized money-center and regional banks offering a spectrum of financial services, not unlike the financial institutions operating in Europe and Asia.

An increase in outsourcing is a byproduct of banking consolidation and the search for cost effectiveness. Many institutions are outsourcing operations, such as transaction processing for automated teller machines and point of sale terminals, network management, and core processing operations. In a 1996 survey, 72 percent of the top 100 banks reported they had outsourced some "core function."[61] This has led to a concentration of core, back-office functions among third party processors, who similarly are experiencing consolidation of their industry. In 1987, there were 24 outsourcing firms with at least 100 bank clients. In 1995, mergers and acquisitions reduced the number of outsourcing firms with more than 100 clients to 14.[62]

5.2 Investment-Related Company Trends

The most notable trend involving the investment sector of the financial services industry has been the rapid increase in the volume of transactions across all exchanges over the last 2 decades. In 1975, 1.3 billion shares were traded on the NASDAQ and 4.6 million shares were traded on the NYSE. In 1996, approximately 138 billion shares traded on the NASDAQ and 104 billion shares were traded on the NYSE.[63]

The large number of shares traded resulted from an increase in the total number of public companies being traded on the exchanges. There are 5,538 companies traded on the NASDAQ and 2,904 on the NYSE. In 1974, there were 2,436 companies traded on the NASDAQ and 1,567 on the NYSE (see figure 5-2). The recent growth in initial public offerings (IPO) has been

---

59 Docket No. R-0841, *Revenue Limit on Bank-Ineligible Activities of Subsidiaries of Bank Holding Companies Engaged in Underwriting and Dealing in Securities.* Board of Governors of the Federal Reserve System.

60 Aaron Elstein, "Goldman Director Says Banks Have Edge in Consolidation Endgame," *American Banker*, February 11, 1997.

61 Liz Moyer, "A Little Help From Their Technology Savvy Friends," *American Banker*, October 1, 1996.

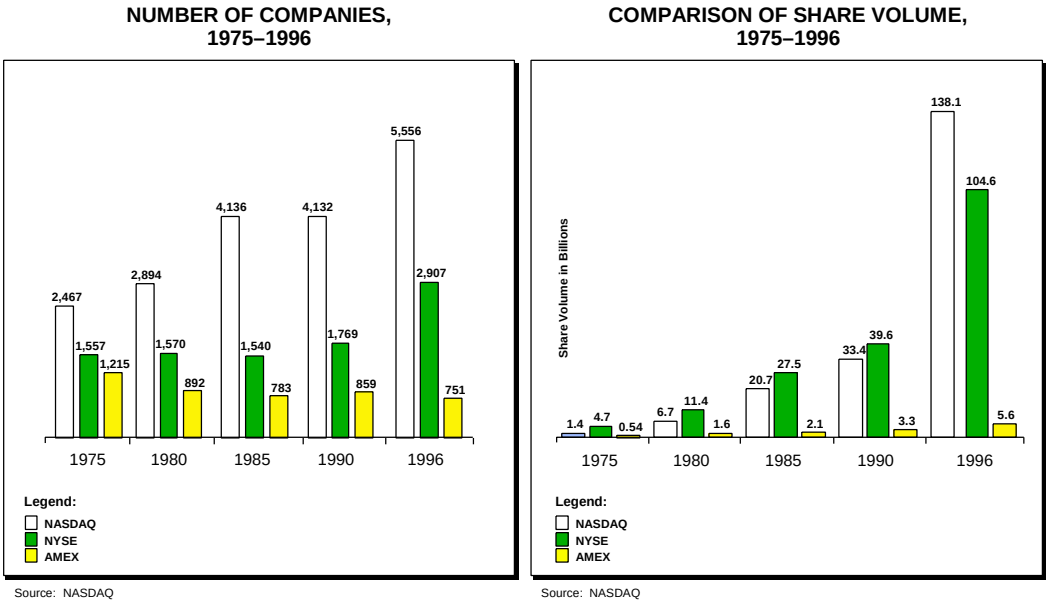
62 Liz Moyer, "Outsourcing Mergers Seen Spawning Price Hikes," *American Banker*, June 7,1996.

63 NASD web site (www.nasd.com).

phenomenal, particularly for NASDAQ securities with 655 IPOs in 1996 compared with 134 IPOs in 1990.[64]

Extensive and continuous technology improvements to the exchanges have made the trading volume levels technically possible. The New York Stock Exchange is near completion of its $125 million technology initiative, the Integrated Technology Plan (ITP). The ITP is the most recent in a series of investments in innovative technology that began with the initial version of the SuperDot automated order-routing system nearly 20 years ago. The ITP follows an investment of $1 billion in the NYSE system during the last 12 years. The ITP will speed the availability of trading information, strengthen the order-management capability on the trading floor, and improve the reliability of the system by enhancing the specialist work stations, the broker-booth support system, and the communications and network infrastructure. The exchange now has the capacity to trade 2.3 billion shares per day.[65]

Figure 5-2. Nasdaq, NYSE, and AMEX Comparison of Number of Companies and Share Volume



In addition, the ready availability of information to both the investment community and the public has increased the aggressiveness in which portfolios are managed. On any given day, the information provided instantly and on a global scale from a variety of providers, such as Dow Jones and CNN, has an immediate and profound effect on the markets.

While the markets may be more active than ever before, enhancements to the clearing and settlement system have improved the stability of the financial services industry. According to the SEC, the market crash of 1987 highlighted a need for a shortened settlement period. During the

64 Ibid.

65 NYSE Web page (www.nyse.com).

week of October 19, 1987, and shortly after, over 50 brokers failed mainly because of the inability of customers to pay settlement obligations and meet margin calls. This failure of customers to meet their transaction settlement obligations or margin calls exposed some clearing firms to financial losses and threatened the entire financial system.

The connection between a crisis in the clearance and settlement system and the financial industry was again highlighted in 1990 by the bankruptcy of Drexel Burnham Lambert Group. Consequently, the SEC adopted the Trade Day Plus Three (T+3) rule, which established 3 business days as the standard settlement time frame for broker-dealer trades, 2 business days less than the previous settlement timeframe (T+5). In effect, the new rule decreases the time between trade execution and settlement, thereby reducing the time during which the value of those trades can deteriorate. Second, T+3 reduces the liquidity risks among derivative and cash markets, and reduces financing costs by allowing investors who participate in both markets to obtain the proceeds of securities transactions sooner. The industry has discussed the possibility of moving to a T+1 settlement time frame but has not established a date for the change.

The consolidation of the financial services industry into full service money center institutions is directly affecting the investment community. And as noted in the preceding section, the lessening of the barriers between banking and investment activities is hastening the convergence of the investment and banking sectors. Those investment companies that are not affiliated with or subsidiaries of a bank holding company are attempting to provide customers with a wider range of financial services by offering services that are functionally indistinguishable from retail banking services. For example, many investment companies offer cash management accounts that function like a traditional checking account.

Globalization is also dramatically affecting the entire investment sector of the financial services industry. Attractive global markets have driven investment in foreign denominated securities as investors and institutions around the world diversify holdings to either mitigating investment risk or maximizing investments. In 1995, $73 billion in international security offerings were made by U.S. issuers and $134 billion in U.S. Treasury securities were purchased by foreign investors.[66] In that same year, 234 foreign companies were listed on the NYSE, more than double the amount 4 years earlier.[67] The need to compete on a global scale will continue to drive consolidation within the investment community and the larger financial services industry.

5.3 Emerging Services

The development of efficient alternative delivery channels for consumer services and core business processes supported by information technology has driven the fluidity and speed in which money and accounts move in the industry.

How and where consumers make contact with their banks are dramatically changing. Interestingly, the geographic location is becoming less important. New delivery methods are far

66 *SIA Factbook*, 1996.

67 *NYSE Annual Report.*

more convenient for the consumer and significantly cheaper per transaction for the bank than transactions that are handled in the branch by employees. A 1996 survey of bank transaction costs points to the clear advantages of automated delivery. A transaction handled by a human teller can cost a bank as much as $2.93, a telephone transaction up to $1.82, an ATM transaction 27 cents, and a PC banking transaction on the Internet, 2 cents.[68] Consequently, technology-based delivery is rapidly growing. U.S. banks report that 50-80 percent of all consumer contacts in 1995 were performed outside the bank lobby.[69]

Although the idea of branchless banks is still considered extreme, the industry is clearly moving toward far fewer banks, fewer branches, and less activity within bank lobbies. Interestingly, size and efficiencies still play a significant role in determining the costs for small versus large banks. Many large banks are introducing new delivery channels or products that cost less than a traditional service. However, banks can not simply abandon the relatively less efficient services. This ultimately increases their costs for delivering services.

Electronic funds transfer (EFT) is the paperless movement of funds between accounts and is firmly embedded into most American consumers' lifestyle. EFT is most often associated with ATMs, point of sale (POS) devices, and ACH, debit, and credit transactions (e.g., payroll, government, mortgages, and insurance payments). The number of ATM machines in the United States has grown from just under 14,000 in 1979 to over 140,000 in 1997. As consumers are becoming more familiar with ATMs, the machines are evolving into full-function processors of cash and noncash transactions (i.e., stamps, tickets, and travelers checks).

Other alternative channels of delivery include 24-hour automated telephone services, supermarket POS terminals, home computers, and the Internet and on-line services. In particular, the on-line banking market is poised for tremendous expansion over the next 5 years. This expansion eventually will fundamentally change the competitive dynamics of the retail banking industry. In fact, a recent survey indicates that both banks and consumers are anticipating vast migration to on-line banking services.[70]

The survey estimates that within 3 years, North American banks will be sponsoring more than 600 Internet sites supporting advanced services such as interaccount funds transfer and electronic bill payment. Moreover, by the year 2000, banks representing more than 40 percent of the deposit base will be offering on-line banking, and the on-line banking market should extend to more than 16 million U.S. households.

Consequently, traditional bank branches staffed with personnel will experience a steady decline. In March 1997, the Bureau of Labor statistics predicted that the number of bank tellers will decline by more than 27 percent by the year 2000. More importantly, service personnel represent overhead that will increasingly become inefficient. The survey indicates that on-line banking customers-because they will tend to be upscale customers-will be almost twice as

68 *American Banker*, Vol. 162 No. 28, p 12, February 11, 1997.

69 Ibid.

70 Booz·Allen & Hamilton, *Consumer Demand for Internet Banking*, July 1996.

profitable as average customers, which translates into almost 30 percent of retail banking profits from on-line services.

The initial model for home banking, involving direct dial-up access from the customer's PC into the bank's host systems, is being replaced by a new model that connects the customer's PC or screen phone to a service provider intermediary such as Meca, which performs bill payment processing or can switch the customer's on-line session into the appropriate electronic network to access various types of account information.

The Internet is the fastest growing sector of the financial/technology marketplace and is widely seen as a "must have" delivery channel for information, services, transactions and commerce. A study issued in March 1997, reported that 18 percent of the U.S. population used the Web in the past month, that 73 percent of Web users accessed the Web for product information, and 53 percent of Web users made a purchase.[71] New electronic payment schemes are constantly being provided to enable electronic commerce over the Internet. Figure 5-3 lists the leading payment schemes that are available or expected in 1997 and 1998.

Figure 5-3. Classification of Internet Payment Systems

CLASSIFICATION OF INTERNET PAYMENT SYSTEMS						
TRADITIONAL MEANS			**ACCOUNT BASED SYSTEMS**			**TOKEN-BASED SYSTEMS**
HOME BANKING/ ELECTRONIC CHECKS	*BILLING SERVICES*	*DIRECT USE OF CREDIT CARDS/DRAFT CHECKS*	*SPECIAL AGREEMENT BETWEEN MERCHANT AND BUYER (SUBSCRIPTION)*	*UTILIZATION OF CENTRAL ACCOUNTING SERVERS*	*DECENTRALIZED SECURE COUNTERS*	
• FSTC electronic check project • BankNet • Quicken, MS Money • Manage Your Money • MECA	• Checkfree • Teleplay • Paylink	• Online checks • Cybercash • SET • Checkmaster • Webcharge/ Webplay • Netmarket • Open Market • CARI • IntenetChecks • Redi-Check	• ClickShare	• GlobeID • Netchex • Netcheque (USC) • Cyberbank • Systemics • Netbill • First Virtual	• Brand's cash • Mondex • CAFÉ • VISAcash	• MagicMoney • ecash • Millicent • PayWord, Micropayments based on iKP • MicroMint • PayMe • Netcash

Up to this point, discussion of trends involving technology in the financial services industry has focused on the enhancement of network-based access to traditional bank services and traditional money. The emergence of stored-valued cards or smart cards, however, creates new money and represents an alternative to government-issued or government-guaranteed financial instruments. In some stored-value systems, the liability representation of the issuer resides

[71] The CommerceNet/ Nielsen study, March 1997.

directly on the card; and, in most systems, a corresponding deposit account is not necessarily maintained for a particular card holder.

This new form of electronic money has significant managerial, financial, legal, and security issues that have yet to be resolved. For example, the untraceability property of some electronic money may create problems in detecting money laundering, electronic counterfeiting, and tax evasion if there is no way to link the payer and the payee. One industry observer succinctly describes the problem, "People have known ways to get money out of banks' information systems for a long time. The problem has been having a place to put it until now."[72] The effect of electronic money on the financial system is still unknown, but studies by the Bank for International Settlements (BIS) and others have warned that digital cash could eventually cost central banks billions of dollars in seigniorage, or float revenue from issuing banknotes.

Smart card technology is also being adopted by the industry for storage of digital signatures and digital certificates that will be used to provide hardware tokens to securely transact electronic commerce. The use of smart card technology in the United States lags Europe. In part, this is attributable to the pervasiveness and reliability of on-line systems. Legislation and attendant regulations for the use of digital signatures and certificates is progressing through many State legislatures, and Federal action is expected as well.

The investment company sector of the industry is directing resources into emerging services to expedite business transactions. The Financial Information Exchange (FIX) is a network-independent protocol designed to standardize how trades and portfolio management systems generate buy and sell orders. Goldman Sachs and Co., Salomon Brothers, Fidelity Management and Research, and others have joined their considerable forces to create and promote FIX.

The investment sector is also developing new delivery channels, most notably through the Internet. Charles Schwab & Co. is considered a leader in the on-line delivery of brokerage services. Approximately 28 percent of all of Schwab's trades are placed through a variety of PC services, including the Internet, proprietary software, and commercial online services. E*Trade, an entirely electronic investment services company, is also experiencing rapid growth. As of December 1996, the company had 112,800 active accounts, up 187 percent from 1995. The company offers access 24 hours per day, through multiple access points (e.g., Internet, Compuserve, America Online).[73]

The Web Browser is emerging as the standard consumer and corporate financial services market interface. Financial institutions are being forced to utilize this interface while maintaining the security of transactions. While the current browser products have the capability to implement strong encryption, the products typically delivered use only 40-bit key encryption. The consensus

[72] William Friel, Science Applications International Corporation, "Comments to Stopping Fraud in Cyber Space Conference," April 17-18, 1997.

[73] E*Trade fact sheet.

among most financial institutions is that 128-bit key encryption provides significantly stronger security and should be the minimum for financial transactions.

5.4 New Technologies

Financial service firms are pouring money into information technology and are expected to continue doing so. Since Bank of America's development and introduction of the Magnetic Ink Character Recognition (MICR) check sorting technology and the Electronic Recording Method of Accounting (ERMA) system in 1959, the financial services industry has been a pioneer in the use of information technology to increase efficiencies and competitiveness. In many ways, the financial services industry exhibits some of the best practices in industry in its use of information technology and, particularly, information security. There are four noteworthy trends in how the industry is adopting technologies.

First, client/server technology is the fastest growing segment of systems development and deployment in the financial services industry. Overall, IT spending is currently experiencing a 6.9 percent compound annual growth rate (CAGR), while client server spending is experiencing a 20.9 percent CAGR. Annual spending on client/server technology will exceed $2.5 billion before the end of the decade.[74] The increased reliance on client/server technology has resulted in far heavier use of wide and local area networks, increasing network managers' concerns about control and security.

It is important to note that mission-critical operations are still overwhelmingly reliant on legacy mainframe processors. And there is no trend to indicate that the financial services industry will be moving away from mainframe processing capability for mission-critical operations. In fact, mainframe usage continues to grow because of an increase in processing volume driven by consolidation of data centers. Worldwide, mainframe-based legacy applications contain over 24 billion lines of code and represent a replacement value of over $100 billion.[75]

Second, the use of data warehouses-informational databases populated by data extracted from operational systems-is growing significantly, especially among the larger institutions. Current information technology-related data warehouse expenditures of approximately $450 million per year by the top 500 banks are expected to grow 30 percent over the next 5 years.[76] The ability to store and manipulate data is becoming a key competitive weapon in the financial services arena and is often used to address a specific business issue, such as product profitability or risk management.

Third, financial institutions are increasingly turning to object-oriented programming to reduce the time it takes to build and modify application software. Object-oriented programming allows developers to build systems using groups of interchangeable "objects" or essentially "mini

74 "Client/server Technology in Banking Update," The Tower Group, 1995.

75 "Legacy System Modernization," The Tower Group, 1996.

76 "Data Warehousing in Banking Update," The Tower Group, 1995.

programs." The result is an increasingly efficient, dependable, and streamlined process for developing new or improved means for customers and employees to access information and services. However, object-oriented programming is a relatively new or immature area, and it will take time before its security implications are understood.

Fourth, the financial services industry will continue to invest heavily in advanced telecommunications technologies, much of it to upgrade infrastructure such as network backbones. Synchronous optical network (SONET), integrated systems digital network (ISDN), asynchronous transfer mode (ATM), and frame relay technologies are being used to ensure the rapid transportation of the large volumes of information inherent to the industry. Many institutions are also investing in fiber optic cable for processor-to-processor connections to ensure high bandwidth capability and availability.

In conclusion, the financial services industry is experiencing a movement of money from the traditionally regulated, FDIC-insured banking environment to an intensely competitive, less regulated environment. Consumers will increasingly benefit from the development of alternative delivery mechanisms for traditional banking type services and investment services. The fluidity and velocity in which money can move within the industry will continue to force institutions to offer new and existing customers a spectrum of financial services at competitive prices. The heavy deployment of and reliance on information technology and telecommunications will proceed unabated into the foreseeable future, underscoring the need for due diligence with respect to security and reliability issues involving all mission-critical networks.

6.0 CONCLUSIONS

At the national level, the financial services infrastructure is very well protected. Security is a fundamental concern throughout the industry. The level of capital investments, staffing resources, and management attention devoted to ensuring both the security of individual transactions and an institution's ability to continue to function throughout a range of contingencies exceeds that evident in just about any other industry. The motivations are strong: the financial impacts of information systems problems can be direct, immediate, and severe.

Beyond the potential for immediate and concrete financial losses is the potential for sustained damage to the institution through loss of customer confidence and trust and, ultimately, the loss of the customer's business. The subgroup observed that financial institutions actually value customer confidence more than the customer's money, which affirms the axiom in banking that the only thing banks really sell is trust.

6.1 Perceptions and Reality

Customer perceptions of an institution's security can be as important as the institution's security measures themselves. The industry has paid for its tendency to avoid disclosing details of its systems and practices through the perceptions fostered by accounts in the media that characterize the situation as being far worse than it is. Virtually no media account of the 1995 Citibank wire transfer fraud incident accurately described how the fraud occurred, and most

implied or asserted that it was a "hack"—that is, an exploitation of some technical vulnerability in the access controls or system interfaces. In fact, the fraud was accomplished in the same way other frauds have been carried out since long before computers were used in financial institutions: by compromising an internal control measure. And the existence of other controls allowed Citibank to quickly detect and track the fraudulent activity, trace it to its source, and stop further losses.

Hackers and even computer security experts themselves also cultivate this perception. "I know a lot of banks who think they are impenetrable, and they are wrong," information warfare author Winn Schwartau has asserted.[77] The authors of *Computer Crime: A Crimefighter's Handbook* state that, "instead of settling for a few thousand dollars in a bank robbery, those with enough expertise can walk away from a computer crime with many millions." Yet the only example of an attack against a financial institution the book cites is a wire transfer fraud attempt against First National Bank of Chicago that involved subversion of telephone authorization procedures, not an intrusion into any computer system.[78]

This perception of the industry has grown in recent years, particularly in light of the increasing presence of financial services institutions on the World Wide Web. In reality, banks view web sites as high risk environments and isolate these sites from internal systems, often completely, and restrict interactions to manual transfer of batch files. Securities firms and industry utilities also take a very cautious approach to connecting to the Internet. Although he criticized banks in his recent survey of Internet web site security, Dan Farmer did note that, "Even if you could break into one of the bank Web sites you couldn't actually steal any money!"[79]

In the Senate's series of hearings on "Security in Cyberspace" in the summer 1996, numerous witnesses testified that financial institutions were at great risk of losses and other serious economic impacts through their reliance on information systems and networks. Commenting on a highly publicized wire transfer fraud against Citibank, Deputy Attorney General Jamie Gorelick speculated, "Imagine what the impact might have been if the intruders were not intent upon stealing funds but on bringing down the entire system…."[80] Popular fiction, particularly Tom Clancy's novel *Debt of Honor*, which depicts a devastating attack on the financial industry created by the introduction of a virus into the industry's computer systems, also leaves the impression that the financial services infrastructure is woefully vulnerable to hacking, insider attacks, and information warfare.[81] None of these assertions are supported by credible evidence: the mere dependence on computers on its own provides the sole basis of these arguments.

---

[77] Reid Kanaley, "Analyst Finds U.S. Treasury, Military Computers Vulnerable to Infowar," www.infowar.com.

[78] David Icove et al, *Computer Crime: A Crimefighters Handbook*, O'Reilly & Associates, 1995.

[79] Dan Farmer, "Shall we dust Moscow? (A Semi-Statistical) Security Survey of Key Internet Hosts," December 18, 1996, http://www.trouble.org/survey/.

[80] In U.S. Senate Permanent Subcommittee on Investigations, "Security in Cyberspace," July 16, 1996.

[81] Tom Clancy, *Debt of Honor*, Putnam, 1994.

No computer system is perfectly secure, and no financial institution can function for long independent of a number of supporting systems and services outside its control. But the business motivations of the financial services industry, extensive regulatory requirements, and the experience of institutions in dealing with a range of natural disasters, system failures, major frauds, and other incidents have led the industry to implement multiple layers of security controls and recovery measures that minimize its vulnerability to all but the most extreme risks. Although institutions are certainly hesitant to disclose information that might undermine customer confidence in the security of their systems, this does not mean that they are not complying with the extensive regulatory reporting requirements. In its report to the "Security in Cyberspace" hearings, the Senate subcommittee's minority staff found no evidence of any financial institution's failure to report or attempt to cover up an electronic intrusion—except the assertions of "numerous information security professionals."[82]

6.2 Natural Disasters and Physical Attacks

As the IATF found in its study of the electric power infrastructure, physical destruction remains a far greater threat to the financial services infrastructure than cyberspace attacks. Although some institutions have implemented impressive physical security protection measures, hardening data centers, building barriers, isolating access points to limit the potential damage from car bombs or missile attacks, many other facilities could easily be knocked out of operation from something as nontechnical as a sewage system backup.

Contrary to popular perception, virtually no facility within the infrastructure represents a single point of failure. The most extreme example might be the trading floor of the New York Stock Exchange or the Chicago Board of Trade. But that does not mean that there is no way to back up or recover the functions of these exchanges. The data centers driving the trading floors have considerable backup and recovery capabilities. The exchanges, the Securities and Exchange Commission, and the Commodities and Futures Trading Commission have studied recovery arrangements in the event of the complete loss of a trading floor.

The systems at the core of the financial services infrastructure, such as Fedwire and CHIPS, operate with on-line backup centers and have the ability to recover essential functions within minutes of an outage affecting the primary site. All the institutions interviewed that were operating very high-volume transaction systems have made huge investments to ensure they can continue processing without interruption through events ranging from the upgrade to a new software release to the destruction of a data center.

One reason the financial services infrastructure is relatively robust is that it has considerable experience in dealing with disasters--natural and man-made, intentional and unintentional. California institutions have been through major earthquakes in 1989 and 1994, and hurricanes and blizzards have forced East Coast firms to operate with minimal staff or exercise

[82] Minority Staff Statement, *U.S. Senate Permanent Subcommittee on Investigations, Hearings on Security in Cyberspace*, June 5, 1996.

recovery plans. The industry also has considerable experience dealing with disruptions to other infrastructures, such as those caused by power outages, central office fires, and cable cuts.

In addition, the industry weathered one of the worst terrorist attacks in recent history. The World Trade Center bombing on February 26, 1993, struck at the industry's heart, affecting the New York Mercantile Exchange and many securities dealers and otherwise disrupting activities throughout Wall Street. Numerous problems with facilities, systems, procedures, and staffs were encountered as firms scurried to recover, and some securities firms' operations were shut down temporarily. However, none of the most critical services were affected, and the effect on the economy as a whole was minimal. Trading continued on the floor of the New York Stock Exchange; payments continued to flow through the facilities of the New York Clearing House and the Federal Reserve Bank of New York. The reality of the destruction provided a much greater incentive for investing in security and recovery than any theoretical exercise or analysis.

Finally, the industry has dealt with a number of major institutional crises within the last decade that have forced it to deal with fundamental issues about its resilience and robustness. As part of its discipline of risk management, the industry has a strong tradition of investigating failures and deficiencies and correcting them.

The increasing velocity of transactions and diminishing time spans within the industry mean, however, that there will be less time available in future to react to these crises. Regulators, the Federal Reserve, and banks had several weeks to respond to the failure of Continental Illinois in 1984, the largest single United States bank failure to date. The response to the failure of Barings Bank in 1994 was worked out over the course of a few days.

To keep the next major bank failure from becoming a crisis overnight, regulators will have to anticipate impacts and have strategies worked out in advance. At a Commodities Future Trading Commission symposium on risk management, Thomas Russo, Managing Director and Chief Legal Officer at Lehman Brothers, supported the utility of contingency plan exercises by stating, "I think having fire drills is a superb idea. I guess it goes down to the basic thing that knowing in advance and having the procedures there so that you have time to breathe."[83]

6.3 Cyber Risks

As perhaps the largest single user of information systems in the United States, the financial services infrastructure potentially represents the largest target for cyber attacks. As this study found, however, the industry has taken extraordinary steps to mitigate its risks in this area. Guided by an overall philosophy of risk management, financial institutions have implemented multiple layers of controls, many of them outside and independent of the information systems themselves.

---

83 Thomas A. Russo, "Dialogue: Risk Management and Internal Controls Concerns from the Perspective of an FCM/Dealer and a Counterparty," Commodities and Futures Trading Commission.

These controls minimize the opportunities for personnel inside institutions to carry out frauds by manipulating data or applications on its information systems. All firms interviewed screened new employees as much as possible, relying heavily on national level checks. Only a few conducted periodic follow-up checks. Concern over potential liabilities limit the information companies will disclose concerning a former employee. There was consistent interest in requests from institutions for obtaining sufficient legal relief to allow more open exchange of employment history information. Maintaining a sufficient level of technical expertise among personnel was another challenge. Another concern raised was the lack of a strong background in or understanding of the fundamental banking or securities business among the newer information technology staff.

Separation of duties and access controls were primary means of deterring and detecting insider intrusions and fraud. Programming and administrative staff generally were not given access to operational systems, and any tools such as compilers and editors that might enable compromise or modification were often stripped from these systems. Transactions involving movement of funds usually require authorization by more than one party and in some cases as many as four. The procedures, protocols, and applications are still highly proprietary, require multiple steps to complete, and tend to be very difficult for an untrained individual to understand, let alone execute successfully.

The same characteristics and controls can be found in most networks involved in the transfer of funds, securities, and other financial transactions. Institutions recognize that use of public networks, whether over voice lines or the Internet, exposes their data and transactions and creates potential avenues for intrusions, and they restrict access to their networks in multiple ways:

- Significant fees and/or capital qualifications for network membership
- Dedicated lines
- Dial-up lines controlled by the network operator
- Dedicated terminals or front-end processors
- Proprietary protocols at the transport and applications layers
- Account IDs, passwords, and authentication procedures
- Use of encryption at one or more layers
- Privileges and capabilities restricted based on roles, capacity, and assets.

The combination of these measures minimizes opportunities for fraudulent activity within networks as well as opportunities for penetrations from outside the networks. The introduction of new delivery channels, particularly dial-up PCs and Internet access, increases the overall exposure of these networks and complicates the problem of maintaining effective access controls. However, most firms appear to be taking a very conservative approach to these channels, isolating them from more sensitive internal systems and screening transactions or limiting credit risks by limiting the value of transactions.

Many of the institutions interviewed were strong advocates of using encryption to ensure the confidentiality and authentication for transactions and for security over public networks.

Customer PINs are currently encrypted in virtually all ATM systems. Application-layer encryption is used in a number of systems to authenticate messages and prevent injection of fraudulent data, and bulk encryption is often used on backbone links. Despite this, however, two concerns with the Federal regulations regarding export of encryption systems in place at the time of the subgroup's interviews were expressed by virtually every institution.

First, most institutions found that even with the existence of a waiver for stronger encryption systems for financial communications, the process of applying for and getting approval to export these systems was slow, complex, difficult to understand, and inconsistently enforced. Some institutions considered the process unworkable; others said it was challenging but workable. None found it anything other than a burden. A few firms with international operations reported the control regulations led them in some cases to buy and build systems overseas to avoid the problem of importing stronger encryption systems than can be exported from the United States.

Second, institutions suggested the net effect of export controls was to artificially constrain the market for encryption products. Financial institutions are among the few commercial users implementing encryption on an extensive basis. A number of firms interviewed believed that the existing export controls or key recovery requirements kept a lot of other customers out of the market. As a result, several firms stated that encryption products they could buy in the United States were more expensive, less powerful, and more difficult to manage than products they could buy overseas.

The Administration's May 8, 1997, announcement of its intention to effectively remove restrictions on export of encryption products designed exclusively for use in financial communications is viewed very favorably by financial institutions and should go a long way to resolve procedural and perceptual issues within the industry regarding encryption.

Institutions strongly supported Federal involvement in some areas of encryption. The need for standards in key exchange and public key infrastructure was seen as opportunities for Federal Government leadership. Several firms saw a need for Federal action to bridge the gap between the current Digital Encryption Standard (DES) and the future Advanced Encryption Standard (AES), particularly in view of recent progress in decryption techniques and the potential for systems capable of breaking DES to become technically and economically viable before AES can be deployed.

The most important information systems challenge reported by the institutions interviewed for this study was not security, but implementing the necessary changes to deal with the year 2000. The tens of millions of dollars invested in security programs in a major institution are dwarfed by the hundreds of millions several institutions said they were spending to fix the year 2000 problem. The risk of malicious code being introduced, particularly given the extensive reliance on outside programmers and the lack of efficient tools for code inspection, was cited repeatedly as a primary concern.

6.4 Cyber Threats

Although financial institutions take more precautions to prevent corruption and disruption of their information systems than perhaps any other industry, they are also among the most guarded in their approach to sharing information about threats and incidents.

One common perception about financial institutions that is accurate is that they are reluctant to disclose details—or even acknowledge the existence—of incidents of internal fraud, regardless of whether a computer is involved. It is important to emphasize that all evidence indicates that conventional forms of fraud-particularly involving checks, credit cards, and compromise of procedures such as in wire transfer systems-vastly outnumber information system frauds in occurrences and impacts.

This does not mean, however, that such incidents go unreported. Internal audits and accounting practices prohibit losses from being "swept under the rug." Reporting in such cases will be extended to the appropriate regulatory authority or a responsible organization such as a credit card or clearing house association. Although loss cannot always be totally eliminated, as in the case of credit card fraud, the industry's rigorous discipline of internal controls means that losses must be accounted for and traced to their source.

Because customer confidence is the highest valued commodity within the industry, however, institutions are extremely reluctant to go beyond the required level of reporting and disclose any information about incidents outside these very limited channels. Most of the institutions the study group interviewed favored informal information sharing mechanisms such as a monthly lunch for information security officers of member banks sponsored by the New York Clearing House, or tightly controlled formal ones, such as the NSTAC's Network Security Information Exchange or the International Information Integrity Institute (I-4).

Institutions were consistently opposed to any additional mandatory reporting process. In particular, banks, having gone through the effort and expense of generating reports related to money laundering to comply with the Bank Secrecy Act and the Foreign Corrupt Practices Act, expressed great concern that the cost of mandatory reporting requirements would far outweigh any potential benefits.

Institutions were also reluctant to share incident information with the Federal Government because, based on their experience with the Financial Crimes Enforcement Network (FinCEN) and others, they found they were generating more information than they ever received in return. The perception that potentially useful threat information was being withheld by intelligence agencies for classification reasons was voiced in a number of interviews. Most institutions stated that their participation in any future information exchange with the Government would be contingent on a guarantee of anonymity and the demonstrated willingness of law enforcement and intelligence agencies to provide more substantial and specific information on threats.

6.5 Summary

The financial services infrastructure of the United States is arguably the finest in the world and is an essential element in the nation's ability to play a leadership role in the world economy.

As this study found, the steps taken within the industry to protect its networks and information systems are extraordinary. The intrinsic value of the funds handled over these systems, combined with the even greater value assigned to maintaining public confidence, has led financial institutions to implement extensive layers of technical and procedural controls that put significant cyber attacks outside the scope of all but a long-term concerted nation-state effort. Physical attacks remain the larger risk for the industry.

7.0 RECOMMENDATIONS

The recommendations of this study are respectively directed toward the President and the financial services industry.

7.1 Recommendations to the President

7.1.1 Threat Information Sharing

The President should assign to the appropriate department or agency the mission of identifying external threats and risk mitigation to the financial services infrastructure and facilitating the sharing of meaningful and timely information between the Government and industry.

7.1.2 Personnel Background Investigations

The President should assign the appropriate department or agency the task of working with the private sector to develop a mutually agreeable solution for effective background investigations for sensitive positions.

7.1.3 Electronic Money and Commerce

The President, in consultation with the financial services industry, should assign the appropriate department or agency the task of monitoring the new/emerging areas of electronic money and commerce, including new payment services.

7.1.4 NSTAC Membership

The President should consider ensuring that the NSTAC continues to have at least one member from the financial services industry.

7.2 Recommendation to the Financial Services Industry

The financial services sector should consider identifying sensitive positions that require extensive screening and skill certification.

APPENDIX A

Financial Services Risk Assessment
Subgroup Members

NSTAC IIG Participants

Mr. Steve Fabes	Bank of America, Chair
Mr. John August	Unisys Corporation
Mr. Clement Chen	Lockheed Martin
Mr. Guy Copeland	Computer Sciences Corporation
Ms. Ernestine Gormsen	GTE
Ms. Mary McNally	Computer Sciences Corporation
Mr. Larry Nelson	AT&T
Mr. Bernard Ziegler	Science Applications International Corporation (SAIC)

Technical Advisors

Mr. Kawika Daguio	American Bankers Association
Mr. Tony Evans	Department of the Treasury
Mr. Craig Hackett	Office of the Comptroller of the Currency
Mr. Frank Kesterman	Department of the Treasury
Ms. Rhonda MacLean	NationsBank
Mr. John Parrrish	Federal Reserve Board

Subgroup Support

Maj Brad Bigelow	National Communications System
Mr. Paul Nicandri	Booz•Allen & Hamilton
Mr. David Owen	Booz•Allen & Hamilton