Chapter 5
International Issues

Dual Regulation

In most countries, banking and telecommunications have both been highly regulated, and institutions that engage in both have borne a double burden. Banking regulation controls the financial services that can be offered and the activities that banks may engage in. Communications regulation controls the technology by which services are delivered and, with respect to many local and long-distance network services, the rates that may be charged. Both affect the classes of customers to whom financial services are offered.

In the United States, the Federal Communications Commission (FCC) generally regulates only communications common carriers, and not the private lines operated or shared by banks. The Federal Reserve Board does not allow bank holding companies to own telecommunications businesses other than one transmitting primarily or only financial or banking data. Telecommunications companies are still regulated at both State and Federal levels, but this regulation generally does not extend to those new activities in which they have begun to participate, and they are not regulated by bank authorities or the Securities and Exchange Commission (SEC). There is relatively little domestic dual regulation.[1] Instead, in the United States, new entities are being created that are not covered by regulations applying to older parallel institutions-for example, it is not clear whether new electronic trading and transactions systems such as Instinct and Globex should be treated as telecommunications systems, securities exchanges, or neither.[2]

In some countries, However, electronic fund transfer (EFT), credit card authorization, and switching for automated teller machines (ATM) are considered telecommunications services, with varying degrees of regulation. The D-Series Recommendations of the Consultative Committee for International Telephone and Telegraphy (CCITT) in the past severely restricted the offering of telecommunications services, although these restrictions were subject to national interpretation. CCITT Study Group 3 has now approved new, liberal recommendations on the use of leased circuits.

Banks often operate cash netting services for multinational corporations. These services enable the corporations to make funds transfers and settlements among subsidiaries around the world, from a personal computer that ties into the banks' networks. Most such systems accommodate some message transmission in the form of instructions or explanations. However, some foreign regulators and postal telephone and telegraphy administrations (PIT's) consider this to be an unlawful messaging activity by the banks, or resale of communications capacity. Some countries discourage shared ATM networks.

In a number of countries, cross-sector regulatory issues are becoming more confusing as both financial institutions and telecommunications systems are deregulated, but at different rates. It may not be clear, for example, whether an on-line transaction is a regulated banking service, a telecommunications service that is regulated in some, but not all, jurisdictions, or an unregulated data processing service. For example, Citicorp allows citizens of the United States to use Citibank ATMs in Japan to withdraw money on deposit in the United States.[3] This raised the issue of whether this is a use of intercorporate leased lines, resale of capacity to a third party (which in Japan requires a license), or provision of a value-added service.

Antitrust regulations or policies that support competition are a problem in several countries, chiefly as they apply to networks operated by groups

---

1 The American Bankers Association notes that some States in the United States have "shown an interest in" regulating credit card authorization and ATMs through State public utility commissions

2 Robert R. Bruce, Jeffrey P. Cunard, and Mark D. Director, *The Telecom Mosaic: Assembling the New International structure* (London: Butterworths, 1988), chapter III, Telecommunications & Transaction Services. The Securities and Exchange Commission has so far declined to regulate them as exchanges but has left open the possibility of doing so in the future

3 Citibank offers an International Citicard that lets travelers overseas use Citibank ATMs to withdraw cash from accounts in the United States (in foreign currency, but with the debited exchange rate shown on screen), and also check their U.S. bank balance or transfer money between accounts. As of now, Japanese customers of Citibank can use their International Citicard in the United States or other countries, but not in Japan, where bank-issued cards carry a magnetic strip that uses local rather than international standards. (Citibank Japan is now redesigning its ATMs.)

of banks. Shared networks may be perceived to reduce competition among banks, or conversely, nonbank suppliers of networks may be viewed as competitors of banks. National authorities may promote legislation with respect to what can or must be shared. On the other hand, if payment systems are seen as part of the larger telecommunications market, where their competitive effects are relatively small, rules designed to assure competition are unlikely to be applied.[4] The Commission of the European Community is now studying institutional and legal aspects of new payments technology.

Although bank networks were studied by the Antitrust Division of the U.S. Department of Justice in the early 1980s, no action was taken and telecommunications regulation has remained limited to common carriers. In the late 1980s, consolidation eliminated nearly half of the ATM networks. The increasing concentration of ATM transactions in a few large networks has again raised the issue of anticompetitive behavior, and both State and Federal antitrust authorities are monitoring the practices of ATM networks.[5]

If payment systems are viewed as telecommunications networks rather than as banking networks, any third party can provide switches to route money transfers from one location to another across national boundaries, although ultimately transfers must show up on the books of depository institutions. In the United States banks now have to compete with money market funds for deposits and nonbank institutions may process and switch monetary debits and credits. Regulators are increasingly less able to monitor, measure, and, perhaps, control money supply. Most importantly, the management of payment risk may become much more difficult.

Shared networks provided by common carriers are subject to telecommunications policies that may not always serve the interests of the financial industry as a whole. For example, SWIFT, cooperatively owned by banks through agreements reached with PTTs around the world, is subject to rate increases for leased lines. Yet SWIFT will be under pressure to remain price competitive as new value-added networks offering electronic data interchange (EDI) make it possible to bypass SWIFT. At the same time, large banks fear that if SWIFT expands into electronic banking services for corporate customers, it will compete with them.

The blurring of traditional industry boundaries is a recurring effect of advances in information technology because it allows organizations to offer new products or perform functions in entirely new ways. These new activities often do not fit older legal or regulatory proscriptions and requirements. New regulatory approaches have been suggested, such as framing regulations and agency jurisdictions around functional activities rather than around industies, institutions, or products-e. g., regulating the activity of lending rather than regulating "banks" or bank credit cards. As noted above, such potential changes should be examined carefully for undesirable effects.

GATT Negotiations

In the early 1980s it often took over a year to get type approval in foreign countries to connect terminal or network equipment to leased circuits. This situation has eased in most countries,[6] but there are still some government restrictions both in industrialized countries and in developing countries that can prevent financial institutions from operating their global networks efficiently. Not all European PTTs are fully committed to providing leased circuits at flat or cost-based rates,[7] a critical factor in offering value-added services and thus in the global competitiveness of U.S. financial institutions.

Large corporations that are heavy users of telecommunications generally argue that a GATT (General Agreement on Tariffs and Trade) treaty must address access to and use of exclusively provided telecommunications services (state-owned systems

4 Marjorie @_teri e, "Public Policy & International Telecommunications Technology in Financial Markets-An Overview," OTA contractor report, February 1992.

5 James J. McAndrews, "The Evolution of Shared ATM Networks," Federal Reserve Bank of Philadelphia, *Business Review*, May-June 1991, p. 3.

6 France, i.e., relaxed restrictions on private networks in its Telecommunications Regulation Law of December 19, 1990. Users may now deploy private facilities to support private networks, although large private networks may still be required to register. Network services were deregulated; restrictions on shared networks such as SWIFT were dropped; and private companies may now sell basic data transport services (e.g., packet switching) to the public.

7 U.S. Department of Commerce, U.S. *Telecommunications in a Global Economy,* report to the Congress and the president of the United States, August 1990, p. 105.

or regulated monopolies) as well as provision of competitive services. An agreement should be flexible enough to accommodate a great variety of regulatory approaches and business needs, and flexible enough to integrate rapid changes in the industry.[8] A U.S. proposed telecommunications annex to GATT would:

- Give users greater freedom to use private line services as they choose,
- Require international private line prices to be based on costs,
- Allow users to interconnect private networks with public networks, and
- Allow users to connect their preferred terminal and network equipment.[9]

These negotiating points generally reflect the needs of U.S. firm-cifi services providers, as expressed in many OTA interviews with bank executives and in a statement by banking representatives to the President of the United States.[10] Financial institutions want their private networks to be interconnected through public switched networks, although treating financial systems as telecommunications systems could raise new issues barely recognized as yet by financial institutions. They want the ability to share use of private circuits, among banks (ATM systems) and between unrelated enterprises (EDI systems), and they want the right to connect leased circuits by whatever equipment is needed. Another key concern is the ability of the customer or supplier to access the financial institution's information systems for data and services, now sometimes prohibited as resale. Financial services providers insist that leased circuits should be priced near costs, so that they are not charged a "tax" to pay for the development of services for the general public. Finally, financial institutions want legal protection for proprietary computer software which they may provide to their customers or suppliers to communicate with the corporation's computer.

Heads of 10 U.S. financial institutions and associations signed a letter to the President of the United States that called for:

> .a strong comprehensive [GATT agreement [that] will increase trade, create jobs in the United States and enhance the international competitiveness of U.S. firms.[11]

Officials of some financial institutions, however, voice reservations about the GATT negotiations; some prefer that the United States rely on bilateral agreements so that they "can work deals [with PTTs] to offer services, sometimes disguised as public services, and this may not be possible under GATT."[12]

The fragmentation of government policymaking in the United States is not a major concern to U.S. financial institutions. "It's an opportunity rather than a problem,' one bank official said cheerfully, because 'we can select the regulator we want to deal with." But it is a problem when the Department of State cannot negotiate bilateral trade agreements because the U.S. Trade Representative considers the issue to be a general trade problem, thus subject to GATT.

Transborder Data Flow Issues

In the view of one banking official, the interplay among financial regulation, telecommunications regulation, and privacy regulation will determine the future of American banking overseas.[13] The possibility of stringent EC privacy restrictions has been a growing concern for U.S. banks, services providers, and large network users because of an EC privacy directive proposed in 1990, which it was feared could disrupt the use of bank-owned global data systems. The directive would have severely limited

8 See "U.S. Industry Proposed Approach for a General Agreement on Trade in Services Applicable to the Telecommunications Services Sector," Submission by the U.S. Council for International Business (to the U.S. Trade Representative), November 1989. This submission was withdrawn for technical reasons but reflects a widely held industry position.

9 U.S. services providers have built enhanced services around proprietary protocols. But some countries, especially Japan, want value-added networks built around CCITT protocols. Marian Barell, Deputy Assistant to the U.S. Trade Representative, in hearings before the Subcommittee on Communications of the Senate Committee on Commerce, Science, and Transportation, U.S. Senate, 100th Congress, 2d Sess. on International Telecommunications Issues, Apr. 19, 1988.

10 Letter coordinated by the Financial Services Group of the Coalition of Service Industries, Inc., Washington, DC, Nov. 25, 1991.

11 Ibid.

12 According to interviews by OTA (non-attribution requested).

13 Michael Nugent, Associate General Counsel, Citicorp, personal communication. Citicorp offers retail financial services; privacy restrictions are a less acute problem for investment and wholesale banking.

the use and transmission of financial and other personal data. The European Parliament, however, raised more than a hundred specific objections to the text of the proposed directive and returned it to the Commission for rewriting. A new version is expected to be released in October 1992, but it is anticipated that the provisions of greatest concern to U.S. banks (and to many European businesses as well) have been greatly modified.[14]

In the mid-1970s transborder data flow issues focused on privacy in the flow of personal data across boundaries. But by early 1980s they had evolved into a broader range of issues including telecommunications policy, economic protectionism, trade barriers, cultural identity, national sovereignty, and security .15

Many American business people believe that what is being called "privacy protection' is a trade issue rather than a privacy issue. They argue that the real goal is the preservation of jobs and the related revenue base for taxation. Governments may use privacy protection to force financial institutions and other large multinational corporations to operate local data centers and keep jobs within host countries. For example, the Canada Banking Act requires that processing of financial data be done within the country; this prevents Citicorp from consolidating its data processing activities in its processing center just across the border in the United States.

However, on the U.S. side, opposition to privacy protection laws may also front for an unstated economic motivation. The laws could tend to promote the deployment of distributed networks in Europe, over the centralized processing approach. Central processing facilities for the most part are equipped with data processing equipment often supplied by U.S. firms such as IBM and DEC.

Legal issues under the privacy umbrella include trade documentation, copyright law, software protection, and the appropriate locus of liability for loss of data. Security and sovereignty issues revolve around possible dependence on foreign suppliers for information and the transfer of high technology to hostile or competitive countries.

Lack of International Monitoring and Oversight

Some banks seek to escape national regulation by locating activities offshore or in countries with different regulatory regimes. International telecommunications networks have unfortunately encouraged this practice. For example, the Cayman Islands (three small islands between Mexico and Cuba) have become a major center of international banking. A British Crown colony, the Cayman Islands were recently reported to hold 548 bank offices.[16] Most of these are 'booking centers" that do all of their work through voice and fax communications and data networks for customers and correspondent banks in other countries. U.S. banks began to use Cayman Island booking centers chiefly to avoid the Federal Reserve System's reserve account requirements.[17] But the banks in offshore havens can also be used for ''laundering' money earned in illegal or unsavory activities.[18] There are said to be over 40 such centers of international banking where modem telecommunications networks allow foreign banks to operate virtually without regulation or oversight.

U.S. banks are subject to laws requiring the reporting of large cash transactions in order to discourage money-laundering.[19] Congress passed legislation that requires the Treasury Department to negotiate bilateral agreements allowing the United States to track cash deposits of U.S. currency in foreign countries for purposes of criminal prosecu-

14 Information provided by the Washington Office of the European Commissions Delegation, Sept. 17, 1992.

15 Edward J. Regan, Vice President, Manufacturers Hanover Tmst Company, in a talk given to the U.S. State Department Bureau of International Communications and Information Policy, at Airlie House, VA, Apr. 8, 1986.

16 Steve Lohr, "Where the Money Washes Up, " *The New York Times Magazine,* March 29, 1992, pp. 27ff. As a British Crown Colony (like Hong Kong), the Islands make their own laws and regulations and the Bank of England has no control over banks there. However, according to the American Bankers Association@ new legislation was enacted in the United Kingdom at the end of 1991 providing for new supervisory responsibilities in the British dependencies.

17 This is not illegal; and Federal Reserve Board of Governors analysts say that because the Board has reduced reserve requirements in the past few years there is now only a minimal incentive to use Cayman Island banking offices to avoid them.

18 According t. Th. *New York Times,* op.cit., footnote 16, Cayman Islands banks were used by Lt. Col. Oliver North to collect money fOr the Iran-Contra arms deal, and by the Bank of Credit and Commerce Internationa(BCCI) to handle its allegedly illegal transactions.

19 This is the practice of moving money from the United States to other countries that do not have such requirements; then, after perhaps moving the money through several "shell" or name-only corporations, wiring it to a U.S. bank account in electronic form not subject to reporting.

tion. Nations that do not cooperate would be subjected to penalties, including loss of the ability to make transfers through Clearing House Interbank Payments System (CHIPS). However, Senator John Kerry (Chairman of the Subcommittee on Terrorism and Narcotics of the Senate Committee on Foreign Relations) has charged that the Treasury Department has failed to negotiate such agreements because the threat of penalties would put U.S. banks at a disadvantage in trade negotiations.[20]

The Basel Committee on Banking Supervision recently adopted stricter minimum standards for supervision of international banking. They recommend:

- Banks opening offices in another country should receive both host and home government approval;
- Regulators in the home country should have the authority to obtain information from foreign bank operations; and
- Bank regulators from countries represented on the Basel Committee (including the United States) should share information.

These recommendations highlight the lack of oversight in the past, but it is far from clear how well they will be implemented or how they can be enforced.

Data Security and Reliability Issues

criminal violations of data security are a serious concern of users of international private networks, although financial institutions are very reluctant to talk about specific instances. Another concern is the possibility of international terrorism. Improved security is one of the reasons often cited by financial institutions for developing private networks. An International Chamber of Commerce Position Paper says:

> In the long-distance network it is difficult to attack specific traffic channels without very expensive apparatus, even if the physical routing of any particular connection is known. . ..whether public switched services or leased lines are used. However, when the traffic reaches the local (or 'serving') exchange office it is concentrated onto discrete routes to the customer's premises. . .[and] is often reasonably physically accessible. . .[and] vulnerable to intercept using relatively inexpensive resources and simple techniques.[21]

On the other hand, some experts now argue that growing security concerns will encourage financial institutions to return to public switched networks. They say that private and shared networks are highly tempting targets for hackers because the financial data is concentrated and readily identifiable, whereas on public networks it is masked by general traffic.[22]

Financial institutions have different approaches to data security on their private networks, including dedicated and well-guarded host computers, recognition procedures, and encryption and authentication technologies.[23] Adequate Security on private networks has become very expensive. Several bank officials interviewed by OTA said that most institutions have woefully inadequate safeguards, both because of the expense and because of general lack of appreciation ''at the Board level" of the risks.

Most financial institutions are much more concerned with data integrity than with confidentiality, and are particularly sensitive to the importance of cost-effectiveness and ease of use in considering security safeguards. Users in some other industries and some parts of government-especially those related to national defense—may have more stringent requirements for confidentiality and may necessarily be more tolerant of higher costs or lessened ease of use. This is the origin of a long-standing dispute over security safeguards and the role of the U.S. Government in developing or mandating them.[24]

The National Security Administration (NSA) was established to unify U.S. signals intelligence operations against foreign communications and to protect

---

20 John Kerry, "A Money-Laundering Loophole," *Daily Telegram, Nov.* 4,1991, p. 15.

21 International Chamber of Commerce, "Communications Network Security: An International Business View" (Policy Statements on Telecommunications, Position Paper 13), pp. 15-16.

22 This opinion was expressed by several network managers in talks with OTA. They were understandably reluctant to be identified.

23 Encryption is encoding text with a unique set of characters (the key) through a mathematical process (the algorithm) to produce a sin-bled or unreadable message so that only a person having knowledge of the key can unscramble it. Authentication techniques make use of newly developed mathematical techniques called public-key cryptography and electronic procedures for providing "digital signatures" to verify the identity of the sender of the message.

24 For a detailed discussion of security technology, see U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information* (Washington, DC: Government Printing Office, October 1987).

U.S. military, intelligence, and diplomatic communications. A civilian agency, the National Bureau of Standards (NBS), now known as the National Institute for Standards and Technology (NIST), played a central role in setting information security standards for civilian government agencies and certifying commercial encryption products. It spearheaded the development of a national standard for cryptography, the Data Encryption Standard (DES). In the 1980s, changing government policies expanded the Federal role, and especially the role of the Department of Defense, in developing information safeguard technology and in certifying standards for encryption and related technologies. National Security Decision Directive 145, in 1984, shifted responsibility for certifying DES-based products from NBS to NSA. In 1986, NSA announced that it would no longer certify DES-based products for government use and would supply its own cryptographic designs for use by U.S. companies and civilian government agencies.

This immediately raised industry concerns about the costs and availability of information safeguards, and about the appropriateness of such a strong role for a military intelligence agency in corporate information security. This dispute has continued, and may have contributed to the slowness of financial institutions to give adequate attention to safeguard technology, as reported to OTA in several interviews.

Errors, as opposed to malevolent interception, are also a serious concern for banks. Human error can be magnified by the speed at which telecommunications work. According to news reports:

> .a minor error by a bank official resulted in a U.K: clearing bank mistakenly paying out, within 30 minutes, more than $3 billion to U.S. and U.K. customers.

This was blamed on a fault in computer software that allowed a payment message to be transferred repeatedly because a date was omitted.[25]

System reliability is a major concern for investment bankers or securities houses; if their systems fail, they will have liability for trades not completed. They will also lose customer confidence, "which is deadly in this business," as a securities house official said. Securities houses are also greatly concerned that data could 'leak' from the network—i.e., be accessed by unauthorized persons to whom it might give unfair advantage in trading. This could subject the firm to SEC penalties for insider trading, as well as result in loss of customers' confidence. Brokers and dealers also must protect their customers' privacy. These concerns are bigger with private or shared networks than public networks because the operator of the network may be held to bear the liability .26

System failure is also a major concern of stock exchanges since the assurance of fair and orderly markets now depends heavily on the proper functioning of their automated systems and telecommunications links. Yet the degree to which stock exchanges and investment banks take steps to reduce risks associated with automated systems varies widely. The attention paid to such risks by national regulatory processes also varies widely .27

Most foreign regulators have given little attention to addressing automation risks and have generally not issued policy guidance on automation control requirements. Both OTA and the GAO have pointed to the need for the SEC and the Commodity Futures Trading Commission to actively encourage the international financial community to address these risks. Five international organizations are now working on the problem: Le Federation Internationale des Bourses de Valeurs, the Group of Thirty, the International Organization for Standardization, the International Organization of Securities Administrators, and the Organization for Economic Cooperation and Development (OECD).[28]

System breakdowns are a more serious problem than crime or hacking for public switched networks. In September 1991 a major telephone system failure in lower Manhattan (Thompson Street) was traced to ''a combination of failures in power equipment and

---

25 Alan Cane, ''Bank Error Leads to $2 Billion Pay-Out to Companies," Financial Times, Nov. 19, 1989.

26 The question of liability for data on private networks is not fully settled, Under UCC 4A the operator must meet "reasonable" standards and reasonable customer expectations of security. In private or shared networks the question of liability is often incorporated in a contract.

27 For a definitive analysis of risks in clearing and settlement mechanisms around the world, see *Study of International Clearing and Settlement, a* study administered by Bankers Trust Company under contract to OTA, 1989, vol. 1; available from National Technical Information Service.

28 GAO, ''Global Financial Markets: International Coordination Can Help Address Automation Risks," IMTEC-91-62-ES, September 1991.

alarm systems."[29] There were big differences in vulnerability to the Thomas Street failure.[30] One bank had concentrated its data processing into two remote centers, using three long-distance carriers and intelligent multiplexer for routing traffic between them. This network lost 25 percent of capacity but suffered no disruption. By contrast, a large securities house lost all connection to the Securities Industry Automation Corporation and could not clear and settle the day's trades over the network. (Failure to have settled would cause it not to be allowed to trade when the market opened the following morning. The securities house was reduced to dumping data onto tapes and ferrying them by automobile to the clearinghouse.) The firm had believed it was fully protected by redundant circuits to its local carrier, NYNEX, but discovered to its chagrin that these circuits all went through one AT&T switch, which failed.

Most financial institutions go to great lengths to have complete redundancy in their own networks, but the public networks to which they are connected sometimes make minor engineering changes without checking to see if this routes ''redundant" circuits through a common switch. Several such cases were related to OTA by Wall Street fins.

The liability of communications carriers for lost or compromised data is emerging as a major issue. Financial institutions would like to bind the public carriers by contract (as is done with private carriers) to guarantee security, but the carriers claim to be unable to assume such responsibility under FCC's tariffing rules. The Bush Administration's position, according to some concerned about the issue, is that the market will take care of this.

Payment System Risks in Shared Financial Networks

A payment system is a system that moves messages that are electronic funds transfer instructions and thereby affects settlements among its members.[31] When monetary value is irrevocably transferred from one party to another, this is called "finality of payment" (i.e., payment in cash). A unique capability of banks is their ability to credit and debit accounts on their books (typically referred to as a "book" transfer) without a physical transfer of cash/currency.

FEDWIRE, operated by the Federal Reserve System, is an electronic payment mechanism that provides finality of payment on an individual transaction basis. CHIPS, operated by the New York Clearing House, has incorporated procedures to assure finality of settlement at the end of the day. SWIFT is considered a communications system rather than a payments system as it moves messages among its members including funds transactions that are subject to settlement by other means. However, Federal Reserve Bank analysts say that for many purposes SWIFT may also be considered a payment system because banks accept instructions sent over it as authoritative.

The use of electronic systems, and especially the reliance on international telecommunications systems for funds transfers, brings with it growing concern about payment system risks. Payment system risks arise in both the U.S. Federal Reserve's FEDWIRE and in private (shared) networks, such as CHIPS and SWIFT FEDWIRE each day transfers billions of dollars between banks. When any bank's payments exceed the balance in its account for some period during the day (i.e., a "daylight overdraft") that is in effect a loan from the Federal Reserve system to the bank-a loan that is paid off at the end of the business day.

Unlike FEDWIRE, which maintains an account in which there are actual funds, CHIPS maintains an electronic book entry account for each participant in the system. Debit amounts in such accounts represent the fact that the participant paid out more than they received. The CHIPS system handles approximately $915 billion per day, and the average total daylight overdraft at the peak of the business day is $45 billion.

If at the end of the day, any bank in a deficit position cannot settle, it has either failed, or been hit

29 Alfred C. Sikes, "A Review of FCC Activities, Accomplishments, and Objectives, " in *Telecommunications,* February 1992, p. 19.

30 The following discussion draws on a number of interviews with financial institutions, which were universally reluctant to be identified in any discussion of security risks.

31 This sections relies heavily on the assistance of Sy Rosen, Vice President for Payment Systems of Citibank, N.A. and a member of the Federal Reserve Board of Governors Large-Dollar Payments System Advisory Group. A basic discussion of payment risk can be found in E.J. Stevens, "Payment System Risk Issues," *Economic Commentary,* Federal Reserve Bank of Cleveland, June 15, 1989; however, this work predates 1990 changes in the CHIPS system to reduce payment risk.

by a severe liquidity problem. Either the Federal Reserve or the other participants in CHIPS or other shared networks are left holding the bag. FEDWIRE operates on the principle of ''irrevocable payment, which means that its funds transfers are final. Therefore the Federal Reserve absorbs the risk that a bank will fail at the end of the day. Private shared networks have no "comparable risk-absorber because payments are not irrevocable. "

In the CHIPS system, since CHIPS acquired settlement finality in 1990, a defaulting bank's net debit position would be covered by an allocation of the other banks on the system in accordance with a set formula. Before 1990, there was no mechanism for covering any resulting illiquidity of those banks and no well-defined risk-assignment law or regulation to determine who should bear the loss. Now there is a collateral pool of U.S. Government securities of about $3.4 billion.

SWIFT messages affect billions of dollars a day by facilitating virtually every international trade and many cross-border securities and foreign exchange transactions.[32] SWIFT is often used to send messages from one country to another. Many countries use its message text standards for payments and thus it can be used as an intermediary to convert from one national clearing system to another.[33] Central banks are increasingly concerned about the scope of settlement failures that could occur on SWIFT'.

The increasing use of international payment networks has given rise to the netting of positions within groups of users. This includes offshore netting centers, such as the Tokyo-based U.S. dollar clearing system and the Private ECU Clearing and Settlement System. The offshore netting schemes are an electronic extension of domestic netting schemes made possible by telematic technology. By reducing the number and overall value of payments between banks, netting improves the efficiency of domestic payment systems and reduces the settlement costs of foreign exchanges.[34] But offshore netting arrangements also are subject to payment risk, and this raises further questions of responsibility and about the role of central banks as lenders of last resort.

In the case of a CHIPS settlement failure it is commonly but unjustifiably presumed that the Federal Reserve might intervene (to the extent, perhaps, of making a short-term loan to banks to cover temporary deficits) .35 With international transfers of funds, the risk becomes greater. It is not known whether foreign central banks would assist foreign CHIPS participants that were subsidiaries of their nation's banks, or whether they would backup participants on offshore netting arrangements. Differences in time zones and bank holidays would also complicate settlement readjustments. .

This leads to a growing danger of systemic risk. When one or more participants in a payment system are unable to meet their obligations, thus causing other participants to default on their obligations, the failures can cascade through a national (and in theory, international) payment system. According to bank authorities,

> Of the various kinds of risk to which banks may become exposed through the accelerated use of the new technology, it is this systemic risk that is the greatest cause for concern.[36]

The Federal Reserve System has taken steps to contain such risks in the United States. U.S. banking authorities have proposed various additional approaches. There is a concern that any national regulations that are viewed as burdensome could result in some banks shifting their participation from onshore to offshore networks to avoid the regulations, or the largest banks might work out bilateral netting arrangements and avoid multiparty networks. After the failure of investment bankers, Drexel Burnham Lambert Group, in April 1990, E. Gerald Corrigan, president of the New York Federal Reserve Bank, set up a committee of commercial and investment bankers to study the implications for the payment system, and to "boost communications among private sector institutions and regulators on

32 Analysts at the Federal Reserve System Board of Governors told OTA that the amount of money moved by SWIFT messages in a day is not known; however, they doubted estimates by other experts of "several trillion dollars. '

33 Greene, op. cit., footnote 4.

34 ''New Report on Interbank Netting Schemes From BIS,' *The World of Banking,* vol. 9, No. 6, November/December 1990, pp. 25.

35 Stevens, op. cit., footnote 31.

36 Bank for International Settlements, *Payment Systems in Eleven Developed Countries* (Chicago, IL: Bank Administration Institute, May 1989), p. 3.

payment, clearing, and settlement issues."[37] This advisory group developed three panels or committees (network operations, contingency planning, regulations), and discussions continue.[38]

At the international level, central banks and industrywide study groups are working on ways to minimize systemic risk and its potential impact on payment systems. A Committee on Interbank Netting Schemes set up by the central banks of the Group of Ten Countries has agreed on minimum standards for the design and operation of cross-border and multicurrency netting arrangements.[39]

As very large multinational corporations establish direct links between their own accounting and those of their banks through EDI networks, and make direct transfers to the debit or credit of other customers and other banks through these networks, payment systems are becoming part of larger networks not controlled directly by bank supervisory bodies. New international mechanisms may be necessary to deal with these enlarged risks and new, non-regulated services providers.

Implications of Electronic Funds Transfer for Monetary Policy

World financial flows have "become largely disconnected from trade flows," says James Brian Quinn, citing estimates that 95 percent of the daily volume of foreign exchange markets are not commercial business but trading between foreign exchange dealers in international banks.[40] Annual money flows over CHIPS or SWIFT ''dwarf world merchandise trade, " and FEDWIRE's volume of transactions far exceeds the U.S. gross national product.

Robert E. Keleher of the Board of Governors of the Federal Reserve System says:

> Revolutions in telecommunications and information processing, deregulation of financial firms, as well as the global integration of financial markets have transformed the environment in which both financial institutions and central banks operate. ***These developments have important implications for monetary policy. They*** have (1) changed the form of financial intermediation, (2) significantly altered the transmission mechanism of monetary policy, and(3) significantly affected the behavior of instruments, indicators, and targets of monetary policy.

Some of these effects come about because of the securitization of corporate and mortgage lending, which was strongly encouraged by lower costs of information processing and transmission, which in turn "dramatically lowered the cost of risk assessment. '[41] Some result from the integration of world financial markets, again encouraged by international telecommunications. A major effect (see box 5-A) is that:

> . . .a monetary policy diverging from the policies in place elsewhere elicits rapid capital flows and sharp exchange rate movements [and causes] changes in monetary policy [to] affect economic activity or prices in different ways than when the economy was less open.[42]

Central banks influence national money supply by reaching a desired operating target through the banking system. (Banks "create" money by making loans; central banks try to control this process by setting reserve requirements and interest rates, and through other procedures.) If the link between the volume of bank balances and the volume of transactions supported by these balances is no longer predictable, it raises questions about the reliability of the central banks' operating targets.[43] A stable relationship between money supply and the monetary base may not be maintained. This may eventually motivate nations to seek an international coordinated approach to control of the money supply.

FEDWIRE and CHIPS together now handle most of the very large monetary transfers that occur in the United States, about $1.7 trillion daily. Automated Clearing House direct deposit and various bank systems handle about one-tenth of that amount daily.

---

37 Jeanne Iida, "Pa$_{ren}$t M&S Getting Fresh Look,'' *American Banker,* Nov. 18, 1991.

38 In November 1991 these panels were dissolved in favor of a committee to study ways of limiting risks to the payment system.

39 'tNew Report. . .", op. Cit., footnote 34.

40 James Brian Quinn, '"I&h.uolo~ in Services: Past Myths and Future Challenge%' Bruce R. Guile and James Brian Quinn (eds.), Technology *in Services: Policies for Growth, Trade, and Employment* (Washington, DC: National Academy of Engineering, 1988), p. 35.

41 Ibid.

42 Ibid.

43 Greene, op. Cit., footnote 4.

Box 5-A—The Currency Crisis

"Wide Currency Crisis Jolts European Unity,"
-Headline, *Washington Post,* September 17,1992

"World's Economies, Now Interdependent, All Suffer Together,"
-Headline, *The Wall Street Journal,* September 17,1992

"The world's currency markets, it seems, are no longer governed by central bankers in Washingtonand Bonn, but by traders and investors in Tokyo, London, and New York, ., ."

Allen R Myerson, "Turnmoil in the Currency Markets,"
The New York Times, September 17,1992.

The European Monetary System (EMS) was designed as a preliminary step in the movement toward a unitary European currency and central bank, the goal of the Maastricht treaty signed by the 12 members of the European Community less than a year ago. The EMS has an exchange rate mechanism that locks in the relative values of national currencies by obligating governments and central banks to take steps (for example, adjusting interest rates) to keep their currencies stable relative to the German mark In a tumultous two day period, under **extreme pressure** from currency speculators and arbitrageurs, the imposed stability collapsed, several national currencies were effectively devalued, and the British pound was withdrawn, at least temporarily, from the European Monetary System.

The conditions for the European monetary crisis were created over several years of economic and political disruptions, by diverging national interest rates, and by other strains attendent on the effort to move toward a unitary currency. But the flows of money through electronically linked currency markets may have strongly contributed to the scope of the crisis and the speed with which it climaxed, and indicated to many observers that money values may increasingly slip beyond the control of central banks and national governments.

SOURCE: "Wide Currency Crisis Jolts European Unity," ***Washington Post,*** **September** 17, 1992, and Allen R. Myerson 'Turmoil in the Currency Markets," **The New *York Times, September* 17,1992, D1.**

Together this is a daily flow equal to 55 times average bank reserve balances, and over one-third of the annual gross national product.[44] Herbert Schiller, describing financial telecommunications systems such as SWIFT and Citibank's GIS, says:

> At the same time as these informational networks have been established, another phenomenon has grown up in the world economy, what ***Business Week*** calls "stateless money—a vast, integrated global money and capital system, ***almost totally outside of all governmental regulation,*** that can send billions of Euro-Dollars, Euro-marks, and other 'stateless' currencies hurtling around the world 24 hours a day. "[45]

Thus telecommunications policy may have a critical role to play in controlling risks associated with the operation of the worldwide financial system, because telecommunications companies are becoming major players in national monetary and payment systems.

44 Elinor Harris Soloman points out that a great deal of money is nowin the form of prepayment embedded in plasticcards ("smart cards," etc.), lines of credit accessible by credit cards, spendablecredits on electronic networks, or electronic float. In moving from cash and paper checks to electronic transfer, the velocity or rate of use of the underlying conventional money has greatly increased. Prior to final payment at the end of each day, much money exists as credits on telecommunications networks and maybe spent several times before net settlement. This will effectively increase with the spread of EDI. Soloman believes that these conditions make many monetary policy levers ineffective. Soloman, "EFT: The Transformation of Money," an address to the Electronic Funds TransferAssociation, Mar. 24, 1992.

45 Herbert I. Schiller, *Who Knows: Information in the Age of the Fortune* 500, (Norwood, NJ: Ablex Publishing Corp., 1981), P. 104.