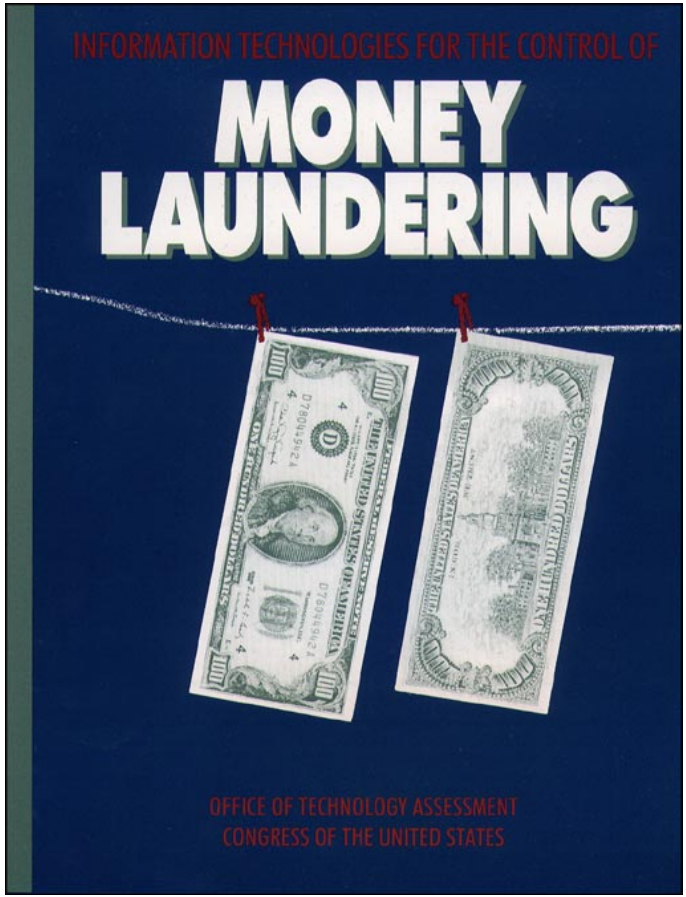
*Information Technologies for the Control of Money Laundering*

September 1995

OTA-ITC-630

GPO stock #052-003-01436-0



**Recommended Citation:** U.S. Congress, Office of Technology Assessment, *Information Technologies for Control of Money Laundering*, OTA-ITC-630 (Washington, DC: U.S. Government Printing Office, September 1995).

# Foreword

The key to control of international crime may depend on cutting off the flow of illegal profits to criminal organizations. It is estimated that $300 billion of "dirty money" may be laundered each year, its origin and ownership obscured as it passes through financial institutions and across national boundaries in an effort to hide and protect it from law enforcement authorities. Criminal organizations, like legitimate businesses, enjoy a swift and nearly risk-free conduit for moving money between countries—wire transfer systems. Illicit wire transfers are easily hidden among the 700,000 mostly legitimate wire transfers that occur daily in the United States, moving well over $2 trillion.

OTA was asked by the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs to assess the proposed use of techniques derived from artificial intelligence research to monitor wire transfer traffic and recognize suspicious transfers. Fully automated computer screening of wire transfers was found to be virtually impossible for technical reasons. However, OTA analysts developed and evaluated a number of alternative configurations of technology that, combined with certain legal and institutional innovations, could greatly enhance the capability of law enforcement agencies to detect and prosecute money launders seeking to exploit U.S. financial institutions and wire transfer systems. Although all of these proposed configurations entail some economic and social costs, including possible diminution of financial privacy, strategies are suggested for minimizing these costs while enhancing the potential usefulness of information technology in control of money laundering.



**ROGER C. HERDMAN**
Director

# Advisory Panel

**Eloy Garcia**
Assistant Special Agent in Charge
Operational Commander

**W. Douglas Johnson**
Assistant Director
Division of Banking
Office of the Comptroller

**Robert MacAllister**
Vice President & Senior Associate Counsel
The Chase Manhattan Bank, N.A.

**Bruce Porter**
Associate Professor of Computer Science
University of Texas at Austin

**Priscilla Regan**
Assistant Professor
Department of Public & International Affairs
George Mason University

**Joel Reidenberg**
Associate Professor of Law
Fordham University School of Law

**Robert Serino**
Deputy Chief Counsel
Office of the Comptroller of the Currency
U.S. Department of the Treasury

**John Stern**
The Francis M. Hipp Building
College of Business Administration
University of South Carolina

**David Vogt**
Assistant Director
Financial Crimes Enforcement Network (FinCEN)

**Sarah Welling**
Professor of Law
College of Law
University of Kentucky

**Note:** OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the advisory panel members. The panel does not, however, necessarily approve, disapprove, or endorse this report. OTA assumes full responsibility for the report and the accuracy of its contents.

# Project Staff

**Peter D. Blair**
Assistant Director, OTA
Industry, Commerce, and
International Security Division

**Andrew W. Wyckoff**
Program Director
Industry, Telecommunications,
and Commerce Program

**Vary Coates,**
Project Director

**David Jensen**
Analyst

**Steven Bonorris**
Analyst

**ADMINISTRATIVE STAFF**

**Liz Emanuel**
Office Administrator

**Karry Fornshill**
Secretary

**Diane Jackson**
Administrative Secretary

**Karolyn St. Clair**
PC Specialist

**PUBLISHING STAFF**

**Mary Lou Higgs**
Manager, Publishing Services

**Chip Moore**
Production Editor

**Cheryl Davis**
Electronic Publishing Specialist

**Chris Onrubia**
Senior Graphic Designer

# Reviewers and Contributors

**Joseph Alexander**
New York Clearing House

**Alfredo Arellano**
Popular Bank of Florida

**F. Robert Armentrout**
Internal Revenue Service
Criminal Investigations Division

**Jim Atchley**
Atchley Systems, Inc.

**Jack Blum**
Lobel, Novins, Lamont & Frug

**Al Brandenstein**
CTAC
Office of National Drug Control Policy

**Vincent Brannigan**
University of Maryland, College Park
College of Engineering

**Gail Brett**
Fedwire
Division of Reserve Bank Operations and Payment Systems
Board of Governors of the Federal Reserve System

**Brian Bruh**

**John Byrne**
American Bankers Association

**Fred Cate**
University of Indiana School of Law

**Michael Corcoran**
Citibank, N.A.

**Frank Curren**
Treasury Management Association

**Michael D'Ambrosio**
Citibank, N.A.

**Kawika Daguio**
American Bankers Association

**Randall Davis**
Massachusetts Institute of Technology

**Jim Dear**
The MITRE Corporation

**Michael Eid**
FinCEN

**John Falvey**
Drug Enforcement Agency

**Carl Felsenfeld**
Fordham University
School of Law

**Richard Fischer**
Morrison and Foerster

**John Forbes**
Office of the Special Agent in Charge
U.S. Customs Service

**Areg Gharakhanian**
National Command and Control Systems
The MITRE Corporation

**Joyce Goletz**
Chase Manhattan Bank, N.A.

**Theodore Greenberg**
Department of Justice

**Edmond Gueguen**
Citibank, N.A.

**Richard Harms**

**Michael Harrington**
The MITRE Corporation

**Patrick Harrison**
Naval Research Laboratory

**Rayburn Hesse**
Department of State

**Michael Hodge**
National Association of Attorneys General

**Cameron Holmes**
Attorney General's Office
State of Arizona

**Sara Jane Hughes**
School of Law
Indiana University

**Charles Intriago**
Alert Publications Partners

**Douglas Jeffrey**
SWIFT

**Carl Jensen**
Racketeering Records Analysis Unit
FBI Labs

**Jeff Jordan**
Office of Enforcement
U.S. Customs Service

**Graham Jordi**

**Thomas Judd**
National Association of Attorneys General

**Louis Kallas**
Office of National Drug Congrol Polisy

**Clifford Karchmer**
Police Executive Research Forum

**Stephen Kroll**
Financial Crimes Enforcement Network (FinCEN)

**Robert MacAllister**
The Chase Manhattan Bank, N.A.

**Gary Marx**
Department of Sociology
University of Colorado

**John McDowell**
Comptroller of the Currency
U.S. Department of the Treasury

**Walter McGovern**
The Chase Manhatten Bank, N.A.

**Greg Meachem**
Federal Bureau of Investigation

**Paul Morawski**
The MITRE Corporation
Artificial Intelligence Technical Center

**Steve Mott**
Cognitive Systems, Inc.

**Howard Mulholland**
Internal Revenue Service

**Joseph Myers**
Office of Legal Counsel
FinCEN

**Jose Ruben Pena**
U.S. GAO

**Kevin Perkins**
Federal Bureau of Investigation

**Gregory Piatetsky-Shapiro**
GTE Laboratories, MS-45

**Graham Pinner**
Australian Transaction Reports and Analysis Centre (AUSTRAC)

**Zelford Platt**
Washington Metropolitan Police Department

**Gregory Polvere**
Internal Revenue Service
Criminal Investigations Division

**Thomas Poplawski**
The Chase Manhatten Bank, N.A.

**Ronald Rice**
Financial Crimes Enforcement Network
U.S. Department of the Treasury

**Neil Robinson**
Office of the Comptroller of the Currency
Division of Enforcement and Compliance
U.S. Department of the Treasury

**Louise Roseman**
Division of Reserve Bank Operations and Payment Systems
Board of Governors of the Federal Reserve System

**Seymour Rosen**
Citibank, N.A.

**Michael Rosenberg**
Office of Strategic Analysis
Financial Crimes Enforcement Network
U.S. Department of the Treasury

**Jeff Ross**
Money Laundering Section
Department of Justice

**Susan Sandler**
Citibank, N.A.

**Ernesto Savona**
National Institute of Justice
University of Trento

**Dan Schutzer**
Citibank

**Ted Senator**
Financial Crimes Enforcement Network (FinCEN)
U.S. Department of the Treasury

**Evangelos Simoudis**
IBM Research
Almaden ResearchCenter

**Richard Small**
Division of Banking Supervision and Regulation
Board of Governors of the Federal Reserve System

**Steven Smith**
Thinking Machines Corporation

**David Sobel**
EPIC

**Malcolm Sparrow**
John F. Kennedy School of Government
Harvard University

**Dan Stepano**
Office of the Comptroller of the Currency

**George Thomas**
CHIPS, New York Clearing House

**George Trubow**
John Marshall Law School

**Viveca Ware**
Independent Bankers Association of America

**Robert Weber**
Office of Enforcement
U.S. Customs Service

**Roger Weiner**
Financial Crimes Enforcement (FinCEN)
U.S. Department of the Treasury

**Alan Westin**
Columbia University

**Mark Westling**
The MITRE Corporation
Artificial Intelligence Center

**Christopher Westphal**

**Steven Wisotsky**
School of Law
Nova University

# Workshop Participants

**The Use of Wire Transfers For Money Laundering**
**June 21, 1994**

**John Byrne**
General Counsel
American Bankers Association

**Jim Dear**
The MITRE Corporation

**Carl Felsenfeld**
Professor
Fordham University School of Law

**Sara Jane Hughes**
Professor
Indiana University School of Law

**Charles Intriago**
Publisher
Alert Publications Partners

**Jeff Jordan**
Office of Enforcement
U.S. Customs Service

**Clifford Karchmer**
Associate Director
Police Executive Research Forum

**Zelford Platt**
Financial Division
Washington Metropolitan Police Department

**Privacy and Confidentiality in Payment Systems**
**September 28, 1994**

**Vincent Brannigan**
University of Maryland, College Park
College of Engineering
College Park, MD

**John Byrne**
General Counsel
American Bankers Association
Washington, DC

**Frank Curren**
Director, Government Relations and Standards
Treasury Management Association
Bethesda, MD

**Stephen Kroll**
Legal Counsel
FinCEN
Vienna, VA

**Vicki Roberts**
Treasurer
Centex Corporation
Dallas, TX

**David Sobel**
Legal Counsel
EPIC
Washington, DC

**Dan Stepano**
Assistant Director, Enforcement and Compliance Division
Office of the Comptroller of the Currency
Washington, DC

**George Trubow**
Director, Center for Informatics Law
John Marshall Law School
Chicago, IL

**Steven Wisotsky**
School of Law
Nova University
Fort Lauderdale, FL

**Information Technologies for Analyzing Wire Transfers**
**September 29, 1994**

**Joseph Collins**
Naval Reseach Laboratory
Washington, DC

**Patrick Harrison**
Naval Research Laboratory
Washington, DC

**Joseph Kielman**
Chief Scientist
Federal Bureau of Investigation
Washington, DC

**Paul Morawski**
Lead Scientist
The MITRE Corporation
Artificial Intelligence Technical Center
McLean, VA

**Steve Mott**
Cognitive Systems, Inc.
Stamford, CT

**Bruce Porter**
Associate Professor of Computer Science
University of Texas at Austin
Austin, TX

**Mark Potts**
Application Specialist
Cray Research Inc.
Calverton, MD

**Michael Rosenberg**
Senior Intelligence Research Specialist
Office of Strategic Analysis
Financial Crimes Enforcement Network
US Department of the Treasury
Vienna, VA

**Ted Senator**
Chief, Artificial Intelligence Division
Financial Crimes Enforcement Network
U.S. Department of the Treasury
Vienna, VA

**Evangelos Simoudis**
AI Center
Research and Development Division
Lockheed Missles & Space Company, Inc.
Palo Alto, CA

**Steven Smith**
Thinking Machines Corporation
Cambridge, MA
Technological Alternatives
February 16, 1995

**Kawika Daguio**
Federal Representative
Operations & Retail Banking
American Bankers Association
Washington, DC

**Jim Dear**
The MITRE Corporation
McLean, VA

**John Falvey**
Staff Coordinator, Financial Investigations
Drug Enforcement Agency
Arlington, VA

**Richard Fischer**
Morrison and Foerster
Washington, DC

**Larry Gilbert**
General Counsel
CyberCash, Inc.
Reston, VA

**Joyce Goletz**
Vice President, Regulatory Compliance
Chase Manhattan Bank, N.A.
Brooklyn, NY

**Richard Harms**
AUSTRAC Consultant
Cupertino, CA

**Cameron Holmes**
Assistant Attorney General
Attorney General's Office
Phoenix, AZ

**Stephen Kroll**
Chief Counsel
Financial Crimes Enforcement Network (FinCEN)
Vienna, VA

**Gregory Piatetsky-Shapiro**
GTE Laboratories
Waltham, MA

**Gregory Polvere**
Internal Revenue Service
Criminal Investigations Division
The Bronx, NY

**Neil Robinson**
Office of the Comptroller of the Currency
Division of Enforcement and Compliance
U.S. Department of the Treasury
Washington, DC

**Seymour Rosen**
Vice President
Citibank, N.A.
New York, NY

**Ted Senator**
Chief, Artificial Intelligence Division
Financial Crimes Enforcement Network (FinCEN)
U.S. Department of the Treasury
Vienna, VA

**Richard Small**
Special Counsel
Board of Governors of the Federal Reserve System
Washington, DC

**Roger Weiner**
Deputy Director
Financial Crimes Enforcement Network (FinCEN)
U.S. Department of the Treasury
Washington, DC

# Acronyms and Glossary of Terms

**ACH**: Automated Clearing House
**ARPA:** Advanced Research Projects Agency (Department of Defense)
**ATM:** Automated Teller Machine
**AUSTRAC:** Australian Transaction Reports and Analysis Centre
**BATF:** Bureau of Alcohol, Tobacco, and Firearms (Dept. of the Treasury)
**BCCI:** Bank of Commerce and Credit International
**BSA:** Bank Secrecy Act (Currency and Foreign Transaction Reporting Act)
**CHIPS:** Clearing House for Interbank Payment Systems
**CIA:** Central Intelligence Agency
**CID:** Criminal Investigations Division (of the Internal Revenue Service)
**CMIR:** Currency or Monetary Instruments Report
**CRF:** Criminal Referral Form
**CTR:** Currency Transaction Report
**CTRC:** Currency Transaction Report-Casinos
**DCC:** Detroit Computer Center (a facility of the Internal Revenue Service)
**DEA:** Drug Enforcement Administration (Dept. of Justice)
**ECPA:** Electronic Communications Privacy Act of 1986
**EDDS:** Electronic Data Delivery System
**FAIS:** Financial Artificial Intelligence System (of FinCEN)
**FATF:** Financial Action Task Force
**FBAR:** Foreign Bank Accounts Report
**FBI:** Federal Bureau of Investigations (Dept. of Justice)
**FinCEN:** Financial Crimes Enforcement Network
**FRS:** Federal Reserve System
**FTR:** (Australian) Financial Transactions Report
**HIDTA:** High Intensity Drug Trafficking Area
**IRS:** Internal Revenue Service (Dept. of Treasury)
**MAFIC:** Multiagency Financial Investigations Center
**NSA:** National Security Agency
**OCC:** Office of the Comptroller of the Currency (Dept. of the Treasury)
**ONDCP:** Office of National Drug Control Policy
**RFPA:** Right to Financial Privacy Act of 1978
**STR:** Suspicious Transaction Report
**SUA:** Specified Unlawful Activity
**SWIFT:** Society for Worldwide Interbank Financial Telecommunication
**TRAQ:** Transaction Reports Analysis Query System
**UNCITRAL:** United Nations Commission on International Trade Law
**USCS:** United States Customs Service (Dept. of the Treasury)

# GLOSSARY

**Artificial intelligence:** The subfield of computer science concerned with the concepts and methods of symbolic inference and symbolic knowledge representation by computers; the attempt to model aspects of human thought on computers.

**Asset forfeiture:** The legal taking of property by government, if it has been used in the commission of illegal acts or represents the proceeds of illegal transactions.

**CHIPS:** Clearing House for Interbank Payment Systems, a wire transfer system (see below) operated by the New York Clearing House.

**Comity:** the voluntary deference of U.S. courts to the legislation of other sovereigns

**Computer matching:** the linking of different computerized databases by unique identifiers

**Cupo account:** A specialized bank account, maintained by a company (often an export/import firm) in a foreign country, where it is allowed to receive and hold a specified quota ("cupo") of U.S. dollars outside of existing currency regulations. May be misused by money launderers.

**Data protection:** similar to fair information practices, data protection principles seek to restore control over personal information held by others.

**Encryption:** Encoding of information to protect privacy or maintain secrecy.

**Expert system:** Knowledge-based systems or computer programs that process data in ways that emulate human experts.

**Fair information** practices: principles governing the collection, use, disclosure, retention, and disposal of personal information.

**Fedwire:** The wire transfer system (see below) operated by Federal Reserve Banks.

**Front company:** An operating business, otherwise or formerly legitimate, that serves as a cover for money laundering operations.

**General warrant or subpoena:** a Constitutionally prohibited non-specific judicial order.

**Integration:** See "money laundering."

**Layering:** See "money laundering."

**Money laundering:** Disguising the origin and ownership of money, often by placing it in a bank, moving it through multiple transactions, and finally mixing it with legitimate funds. These steps are known respectively as placing, layering, and integrating the money. In this report, "electronic money laundering" indicates that wire transfer of the funds constitutes one or more steps in the laundering process.

**Offshore banking, or offshore financial center:** Agglomerations of banks and other financial institutions outside of the jurisdictions of major centers of economic activity such as the United States, in order to avoid the regulations or tax regimes of the larger countries while serving the needs of their institutions and investors. The offshore financial centers offer various advantages such as bank secrecy, low or no tax on interest income, looser regulations, etc.

**Payable-through account:** A specialized bank account, maintained by a bank of one country in a bank of a foreign country for the convenience of the first bank's customers, who are given signature authority to conduct transactions using the account. Often misused by money launderers, with or without the complicity of the bank maintaining the account.

**Placement:** See "money laundering."

**Profile:** A set of descriptors that allows recognition or categorization of subjects.

**Secondary use:** manipulation and use of information beyond the purpose for which it was originally gathered.

**Shell company:** A corporation that exists only formally, incorporated as a cover for illegal operations such as money laundering.

**Smurf:** To divide large illicit bank deposits into several transactions, each under $10,000, so that they will not become the subject of a Currency Transaction Report, as required by the Bank Secrecy Act. Smurfing is more formally known as structuring (a deposit).

**Structure** (a deposit): See "smurf."

**Subpoena:** compulsory process requiring the production of records or testimony; resistance to which may be punished by judicial proceedings.

**Threshold account:** A specialized bank account that allows funds to be automatically wire transferred to a specified location once deposits into the account have reached a specified amount. Used by corporations to periodically concentrate revenue from several subsidiaries; may be misused by money launderers.

# Contents


**1 Electronic Money Laundering 1**

Money Laundering—What Is It? **2**
"Placing" Dirty Money **3**
Layering: Strategies for Hiding Dirty Money **8**
The Global Underground Economy **10**
Professionalizing Money Laundering **12**
Nonbank Money Transmitters **15**
The Outlook **17**

**2 The Mechanisms of Wire Transfer 19**

Moving Money: Book Transfers and Electronic Transfers **19**
Uses and Users of Wire Transfers **20**
Money Center Banks: Gateways to Wire Transfer **23**
Retrievability of Wire Transfer Records **24**
Electronic Funds Transfer Systems: Digital Pipeline for Money **25**
New Wire Transfer Regulations **32**

**3 Money Laundering and Law Enforcement 35**

Laws and Regulations **35**
Federal Agencies' Roles and Responsibilities **39**
State Law Enforcement **42**
The Financial Crimes Enforcement Network (FinCEN) **43**
Summary **48**

**4 Technologies for Detecting Money Laundering 51**

Basic Technologies **51**
Detecting Money Laundering **63**
Findings **74**








## 5 Privacy and Confidentiality 75

Constitutional and Legislative Perspectives on Financial Privacy **79**
The Privacy of the Individual and The Control of Crime **87**
The Confidentiality Interest of the Corporation **92**
Conclusions **99**

## 6 International Issues 101

Access to International Wire Transfer Information **102**
International Law Enforcement Efforts **111**
The Struggle of Sovereigns **117**
Conclusion **118**

## 7 Conclusions and Policy Options 119

Money Laundering and the World Economy **120**
What Would a Computerized Monitor Look For? **124**
Designing Systems for Use by Law Enforcement **124**
Privacy and Corporate Confidentiality **125**
International Considerations **129**
Technological Configurations **133**
Options **136**

# Electronic Money Laundering 1

Crime can be highly profitable. Money generated in large volume by illegal activities must be "laundered," or made to look legitimate, before it can be freely spent or invested; otherwise, it may be seized by law enforcement and forfeited to the government.[1] Transferring funds by electronic messages between banks—"wire transfer"—is one way to swiftly move illegal profits beyond the easy reach of law enforcement agents and at the same time begin to launder the funds by confusing the audit trail.

The Senate Permanent Subcommittee on Investigations, in January of 1994, asked OTA to assess the feasibility of using computer techniques derived from artificial intelligence (AI) to monitor the records created by international wire transfers and thereby detect money laundering.

Wire transfers of illicit funds are readily concealed among wire transfers moved by electronic funds transfer sytsems. Each day, more than 465,000 wire transfers, valued at more than two trillion dollars, are moved by Fedwire and CHIPS, and an estimated 220,000 transfer messages are sent by SWIFT (dollar volume unknown). The identification of the illicit transfers could reveal previously unsuspected criminal operations or make investigations and prosecutions more effective by providing evidence of the flow of illegal profits.

Until now, it has seemed impossible to monitor or screen wire transfers as they occur, both because of the tremendous volume of transactions and because most wire transfers flow through fully



[1] Legitimately earned money that has been concealed from tax authorities is also at risk of seizure.

automated systems with little or no human intervention.[2] As a possible way out of this impasse, it has been proposed that a computer-based system be developed to screen wire transfers on a continuing basis. Such a system would be designed to use advanced techniques derived from artificial intelligence research to recognize and flag unusual events or recurring suspicious patterns, for investigation. This proposal was developed within law enforcement, defense, and intelligence agencies concerned with drug trafficking, terrorism, espionage, and illegal arms trade.[3]

The OTA assessment concluded that the original concept in its simplest form—continuing, real time monitoring of wire transfer traffic, using artificial intelligence techniques—is not feasible. There are, however, several ways in which information technology may be applied to wire transfer records to support and enhance law enforcement against money launderers. This report presents several technological scenarios, or alternative technical configurations and institutional embodiments of information technology. The legal, economic, and social implications of each scenario are identified, to provide a framework for consideration of policy options for the Congress.

This chapter describes modern money laundering, its relationship to drug trafficking and other crimes that operate on a national and international level, its importance to law enforcement, and the role played by banks in control of money laundering.

## MONEY LAUNDERING—WHAT IS IT?

To launder money is to disguise the origin or ownership of illegally gained funds to make them appear legitimate. Hiding legitimately acquired money to avoid taxation also qualifies as money laundering.

Federal agencies estimate that as much as $300 billion is laundered annually, worldwide.[4] From $40 billion to $80 billion of this may be drug profits made in the United States. A multinational Financial Action Task Force estimated that about

---

[2] It is also extremely difficult to find wire transfer records after the fact, in order to reconstruct the flow of money, unless the name or account number, the time and place of origin, or other specific characteristics are known. In addition, either a search warrant or a subpoena is generally required for law enforcement agents to view domestic wire transfer records in electronic form; international wire transfer records (in the United States) will soon be available on request.

[3] The U.S. Customs Service's Financial Division began work on a system in the mid-1980s to analyze Currency Transaction Reports (CTRs). When the Financial Crimes Enforcement Network (FinCEN) was established by the Department of the Treasury in 1988-89, the Customs group involved in this development were transferred to the new agency, which then developed the Financial Artificial Intelligence System (FAIS) now used for targeting suspicious patterns in the CTR database. Other work on artificial intelligence (AI) systems for money laundering control was funded by the Advanced Research Projects Agency (ARPA) in 1991, according to Dr. Al Brandenstein, now director of the Counternarcotics Technology Assessment Center in the Office of National Drug Control Policy (ONDCP), in discussions with OTA, June 1994. ARPA's interest in money laundering was primarily related to terrorism and illegal sales of arms rather than drug trafficking. The agency funded several projects to explore the feasibility of using artificial intelligence techniques to detect electronic money laundering, but when its budget was tightened in 1992, these projects were dropped. Several research contractors, including MITRE Corporation, which had been contractor to ONDCP and to the Drug Enforcement Administration, have continued to push for further development in this area. MITRE analysts were instrumental in bringing the concept to the attention of congressional committees, including the Permanent Subcommittee on Investigations of the Senate Government Affairs Committee, as a potentially powerful tool for attacking drug traffickers. Intelligence agencies are believed to use techniques based on artificial intelligence for some kinds of pattern recognition and analysis related to national security.

[4] This is the estimate used by the international Financial Action Task Force (U.S. Dept. of State (Narcotics) Fact Sheet, "Combating Drug Money Laundering," March 2, 1992). It appears that this estimate was first generated by one U.S. government analyst as "mostly a guess," and has since been accepted as reasonable by other agencies, including the International Narcotics Matters unit within the U.S. Department of State. The Department of the Treasury declines to provide an estimate, beyond saying that the volume "is very big." Approximately $100 billion is thought to be drug-related laundering, the rest is thought to be tax evasion, or proceeds of other crimes including securities manipulation. See also National Institutes of Justice, *Research in Brief*, September 1992, p. 1. Colombia estimates that $1 billion to $2 billion in drug profits comes into its economy from foreign sources.

$85 billion per year could be available for laundering from drug proceeds alone.[5] However, this and other estimates of the scale of money laundering must be viewed skeptically. The official estimates are derived from a mix of experience, extrapolation, and intuition; the hard evidence to support them is limited. No one can be sure how much money is laundered (see box 1-1 and box 1-2).

Money laundering has attracted growing attention in the last decade, in part because of its importance to drug trafficking. It has proven nearly impossible to interdict the flow of drugs into the United States or to halt their distribution within the country. Those most responsible for the international drug trade—high-level drug lords—are the least likely to be apprehended; they are often overseas, out of legal reach. Possibly the most effective way to discourage drug suppliers, therefore, is to cut off the flow of their profits and seize their assets.

Money laundering is not, however, limited to drug trafficking. It is associated with nearly all kinds of "crime for profit," including organized crime and white collar crimes, such as the real estate fraud and savings and loan abuses that marked the last decade. One economist lists a number of other reasons (not all of them criminal) for wishing to hide money: [6]

- to prevent the erosion of business and personal asset values through legal means (such as law suits or divorce proceedings);
- tax evasion, either personal or corporate;[7]
- capital flight from one country to other countries, triggered by adverse changes in economic, political, and social conditions;
- securities law violations, especially insider trading;
- government undercover activities such as spying and support for "freedom fighters";
- smuggling of contraband.

Until 1986, money laundering itself was not illegal apart from the underlying (or *predicate*) crimes that it helped to conceal. Money laundering was first defined as an independent crime in the Money Laundering Control Act of 1986, codified at Sections 1956 and 1957 of Title 17 of the U.S. Code. The penalties include 10 to 20 years in prison and substantial fines.[8]

In 1988, Congress extended the use of civil asset forfeiture to money laundering. As a civil law process, forfeiture requires a lower standard of proof and carries reduced procedural guarantees compared to criminal prosecution. Critics argue that this may lead prosecutors to pursue money launderers rather than "real" criminals, whose actions directly create victims. Law enforcement officials, however, insist that they are properly targeting those who manage, control, and profit by crime, yet insulate themselves from direct contact with it.

## "PLACING" DIRTY MONEY

Law enforcement officials describe three steps in money laundering:

- placement—introducing cash into the banking system, or into legitimate commerce;
- layering—separating the money from its criminal origins by passing it through several financial transactions, for example, transferring it

[5] Financial Action Task Force on Money Laundering, *Report,* Paris, Feb. 7, 1990. The task force was created during the 15th annual Economic Summit in Paris, in 1989, as described in chapter 6.

[6] Ingo Walter, *The Secret Money Market* (New York: Harper & Row, 1990), chapter 1.

[7] In some cases, when dirty money is legitimated or integrated by investment in real estate or legitimate businesses, "the principals may willingly pay taxes on their profits (or file returns that use allowable deductions to avoid taxes)." In other situations, complete avoidance of taxes is an important objective." (National Institutes of Justice, *Research in Brief,* September 1992, p. 1.)

[8] The average sentence imposed on convicted money launderers by federal judges in FY 1992 was 46.1 months, as compared with an average sentence for drug trafficking of 89.4 months or racketeering of 106.4 months. "Convicted Launderers Fit White-Collar Profile," *Money Laundering Alert,* December 1994, p. 2, quoting from a 1993 report by the U.S. Sentencing Commission.

## BOX 1-1: Estimating Money Laundering

The Financial Action Task Force on Money Laundering used three indirect methods of estimating the amount of money laundering:

1, Extrapolation based on estimation of world drug production, This method involves many uncertainties, including the following:

- global crops of opium poppies, coca shrubs, cannabis, etc.,
- internal consumption and export of drugs in each of the producing countries,
- clandestine laboratory production of psychotropic substances,
- street prices of drugs,
- the role of each kind of drug in the generation of proceeds and the level at which proceeds are generated (retail, traffic, wholesale distribution, production, etc.), and
- financial flows within individual countries.

2. Extrapolation from the consumption needs of drug users, Because consumption of drugs such as heroin and cocaine is illegal in many places, both reporting and sampling are unreliable,
3. Extrapolation from seizures of drugs by law enforcement, using a multiplier usually ranging from 5 to 20 percent depending on the drug and the country,

SOURCE, Financial Action Task Force on Money Laundering, Report, Paris, Feb. 7, 1990, pp. 6-8

into and then out of several bank accounts, or exchanging it for travelers' checks or a cashier's check;

- integration—aggregating the funds with legitimately obtained money or providing a plausible explanation for its ownership.

Profits from organized crimes (drugs, gambling, racketeering, and prostitution) are commonly in the form of cash, mostly in small denominations, that must somehow be slipped into the banking system or the regular stream of commerce before it can be safely spent in this country or sent up the rungs of the criminal hierarchy to those demanding their profits.[9]

Street sales of drugs are usually conducted with $5 or $20 bills. A million dollars in $20 bills weighs 111 pounds, in $5 bills 444 pounds.[10] Both convenience and, more importantly, the risk of having the money found and seized by police or by other criminals, make it desirable to take the currency to a bank and either convert it into a negotiable instrument (such as a cashier's check), or wire transfer it to another location.

In 1970, many U.S. banks would accept large cash deposits without question, even from otherwise unknown customers—at times receiving large trash bags stuffed with currency. Money laundering was not illegal. The 1970 Bank Secrecy Act (BSA) required only that financial institutions report currency transactions of over$10,000 to federal law enforcement agencies for possible investigation. This did, however, create an ex-

[9] The recurring cash surplus in certain Federal Reserve Districts, resulting from an abnormally high volume of cash deposits, has been discussed as a possible indicator of money laundering, but this turns out to be unreliable. Miami, Los Angeles, San Antonio, Jacksonville, and El Paso consistently report cash surpluses. Some seasonal peaks in cash surplus in San Antonio were apparently associated with the State Fair. New York City always shows a large cash deficit, and some cities show wide swings. For example, San Francisco, Philadelphia, Denver, Nashville, and New Orleans had large surpluses in early 1994 but large drops at mid-year. "Mystifying Fed Currency Surpluses Show Major Shifts, ''Money *Laundering Alert,* August 1994, p. 4.

[10] General Accounting Office, *Money Laundering: The U.S. Government is Responding to the Problem,"* GAO/NSIAD-91-130. May 1991. p. 13.

## Box 1-2: Estimates of Drug Profits

The Office of National Drug Control Policy (ONDCP) recently published estimates of the amount spent on illegal drugs in the United States. The study, produced by Abt Associates under contract with ONDCP, estimates that Americans spent $49 billion on illegal drugs in 1993. Of that, about $31 billion was spent on cocaine, $7 billion on heroin, $9 billion on marijuana, and the remaining $2 billion on miscellaneous other drugs. [1] The study estimates that spending on illegal drugs has declined steadily since 1988, when spending was estimated to be over $64 billion. The primary causes for the decline include a decrease in the number of users of cocaine and heroin and a decrease in the prices of those drugs since 1988.

Estimating the amount spent on illegal activities is fraught with difficulty, but the ONDCP study's estimates appear quite credible. They track closely with independent estimates made by OTA prior to obtaining the study, and they are based on more precise data. They are probably the most easily estimated portion of total money laundering in the United States, because other activities (e. g., fraud, extortion, etc.) are not subject to the same levels of detection and data gathering.

However, drug spending estimates are difficult to make because few statistics on use and prices are known with certainty. Instead, estimates must be made based on surveys and law enforcement data which are error-prone and uncertain but provide starting points for estimates of drug use and fairly reliable evidence of drug prices. The known data can be combined with additional medical and economic knowledge. For example, there are upper bounds on the amount of drugs that a single individual can consume and on the amount of money that an individual can spend each day on illegal drugs.

Part of the ONDCP study evaluated drug demand in order to estimate drug expenditures. Consumption estimates were based on data from several sources: 1 ) the National Household Survey on Drug Abuse (NHSDA), which surveys individuals about their drug use; 2) The Drug Use Forecasting (DUF) program, which questions a random sample of arrestees in central city jails and lockups about their drug use and conducts urinalysis; 3) the Drug Abuse Warning Network (DAWN), which reports on

[1] The comparatively large amount spent on cocaine is due to the relatively large base of users of concaine (estimated at over two million hardcore users and about four million occasional users) as compared with heroin and the relatively high price of cocaine as compared with marijuana.

*(continued on next page)*

pectation that banks would not knowingly cooperate with money launderers (see box 1-3).

Even after the BSA was passed, many banks were reluctant to refuse customers bringing in large amounts of cash—they did not like to turn away business, and in addition they feared offending legitimate customers by mistake. Bank regulators generally did not aggressively check bank procedures for BSA compliance.

In 1984, however, after the Presidential Commission on Crime called attention to the increasing seriousness of money laundering, the Federal regulators began to press for better compliance. The Bank of Boston was fined $500,000 for failing to report an international transfer of funds; other banks were also fined or given warnings. Compliance improved dramatically. The number of Currency Transaction Reports (CTRs) increased rapidly, to 10,765,000 in FY 1994.[11]

Banks were also required to report "suspicious transactions" to law enforcement agencies, for ex-

[11] A revised form of the CTR will be issued in 1995.

## BOX 1-2: Estimates of Drug Profits (Cont'd)

tens of thousands of emergency room admissions for drug-related conditions; and 4) the System To Retrieve Drug Evidence (STRIDE), which makes estimates of drug prices based on the experiences of street officers and undercover agents, By using these data sources, the study estimated the total number of users of each drug, how much of each drug users consume, and the street prices of each drug,

In addition to estimating drug demand, part of the ONDCP study evaluated drug supply. It did this only for cocaine, because reliable figures were not available for other drugs, The cocaine supply estimate was based on: 1 ) State Department figures on land under cultivation in major coca producing countries, crop yields, and eradication efforts; 2) data from law enforcement agencies on seizures, and 3) data from the Drug Enforcement Agency on conversion rates at various stages of cocaine processing, This information was combined through a simple model of coca cultivation, cocaine processing, and drug shipment. The resulting estimate was in close agreement with the demand-based estimate,

The study's estimates are large, but given the estimated number of users in the United States, even modest expenditures can multiply quickly. For example, the study estimates the number of hard-core cocaine users at just over two million and puts the median users' weekly expenditures at $221 This produces total annual expenditures of $23,3 billion (the remaining $7,5 billion of estimated cocaine spending is by occasional users),

Not all drug use produces money that must be laundered through sophisticated means Not all use of illegal drugs generate money that must be laundered at all. Some drugs are kept by dealers for personal use, some drugs are given to users who assist dealers, and some drugs are exchanged for other services (e. g., crack cocaine is sometimes exchanged for sex), The ONDCP study estimates that such "income in kind" amounts to $3 billion to $5 billion annually, although such estimates are highly uncertain, Not all currency generated by drug sales would be laundered using electronic means Some funds are used directly by dealers to pay for services and non-drug goods (e.g., living expenses, transportation, and firearms)

SOURCE: Office of National Drug Control Policy, *What America's Users Spend on Illegal Drugs, 1988-1993,* prepared by William Rhodes, Paul Scheiman, Tanutda Pittayathikhun, Laura Collins, Vered Tsarfaty, Abt Associates Inc. (Washington, DC Spring 1995)

ample, when a large cash deposit seems inappropriate from a given customer, or when other unusual circumstances mark the transaction as questionable. One simple way to do this is by checking one block in the CTR for that transaction. Alternately, banks can directly notify a law enforcement agency. About 0.5 percent of CTRs are marked "suspicious,"[12] and only about 5 percent of suspicious transaction reports now involve wire transfers as one of the reasons for suspicion. [13] The Criminal Division of the Internal Revenue Service (IRS) is changed with checking on suspicious transactions, but does not have enough investigators to do this consistently or quickly. Therefore, reports of suspicious transactions have in the past been used more often to support an investigation already underway than to initiate an investigation. [14]

Banks, or bank examiners, also have the duty of filing Criminal Referral Forms (CRFs) when they believe they have detected a potential money laun-

[12] FinCEN response to inquiry (questionnaire) by INTERPOL-USNCB (Ms. Shelley G. Altenstadter, Chief), March 24, 1994.

[13] According to experts at OTA's workshop on wire transfers, June 21, 1994.

[14] According to experts at OTA's workshop on wire transfers, June 21, 1994.

## BOX 1-3: Currency Transaction Reports (CTRs)

Between 1970 and April 1983, there were 498 million Currency Transaction Reports (CTRs) filed; thereafter, the rate greatly increased, growing by nearly 13 percent per year from 1987 to the present. (Note that inflation averaged 3.3 percent) In 1994, there were 10,765,000 CTRs filed. Until mid-1993, the volume of CTRs filed far overwhelmed any attempt to Investigate all of them and made it difficult to locate specific records needed to complete an investigation or to provide evidence in prosecutions. Now, the Financial Crimes Enforcement Network (FinCEN), a law enforcement support unit in the U.S. Department of the Treasury, uses the FinCEN Artificial Intelligence System (FAIS) to process every CRT. By relating this information to other BSA records, suspicious subjects can be targeted for Investigation.

The requirement for a CTR applies to every transaction over $10,000. This includes cash deposits, withdrawals, and purchases of financial Instruments by individuals, but it also includes deposits (and other transactions) carried out by businesses Banks must file CTRs for the regular deposits of retail goods and services vendors such as bars, grocery stores, liquor stores, restaurants, laudromats, and gas stations whose customers often pay m currency.

Over 98 percent of CTRs are filed by banks, ' although other financial institutions, such as money exchangers, are also required by law to file The banking Industry maintains that this imposes a heavy and unnecessary burden on banks In 1993, reportedly, the 368 largest banks (those with assets of over $1 billion) filed 4.5 million CTRs, and this compliance was estimated to have cost the banks $72 million dollars.[2] The American Bankers Association says that it costs a bank from $3 to $15 to file a CTR, depending on the size of the bank, its overhead, and whether its system is manual or automatic. The IRS says it costs the federal government $2 to process and store each one.

Ninety percent of the businesses that are the subjects of CTRs are involved in 50 or fewer CTRs a year, or about one a week, while just over half of one percent filed 400 to 1000 CTRs a year, or better than one a day.[3] About 30 to 40 percent of the currency transactions are regular and routine deposits by well-known retail stores or chains.[4] Banks have the power to establish exemptions for regular customers of this kind, and so eliminate many of these routine filings, but most do not. Banks say that they are reluctant to use their exemption power for fear of penalties if they err on the side of exemptions. Also, most large banks have automated the CTR filing in such a way that exercising the exemption is more expensive (for the bank) than filing the CTR.

The CTRs are sent to six federal and state law enforcement or regulatory agencies and are processed in two databases. one maintained by the Internal Revenue Service in Detroit and one maintained by the U.S. Customs Service in Virginia Because of the huge volume of CTRs, access to these data is cumbersome. The data can be used in building a case or as prosecutorial evidence more easily than in identifying money laundering activities not already under active Investigation

---

[1] General Accounting Office (GAO), *Money Laundering: Characteristics of Currency Transaction Reports Filed in Calendar Year* 1992, GAO/GGD-94-45FS, November 1993

[2] John Byrne, General Counsel, American Bankers Association (ABA), compliance cost was extrapolated from a survey of 10,000 ABA member banks in 1990

[3] GAO, op. *cit.,* footnote 1

[4] Henry Wray, Director, Justice Issues, Government Division, GAO, statement in "Federal Governments Response to Money Laundering," Hearings before the Committee on Banking, Finance, and Urban Affairs U.S. House of Representatives, 103rd Cong., 1st Session, May 25 & 26, 1993

SOURCE: Off Ice of Technology Assessment, 1995.

dering violation, regardless of the size of the transaction.[15] These reports, which may be accompanied by a direct telephone notification to bank regulators or to Treasury's Office of Financial Enforcement, are supposed to be based on reasons more substantial than the mere size of a cash transaction.

Because of the Money Laundering Suppression Act of 1994, however, new suspicious transaction reporting regulations will be issued sometime in 1995. A new form will be required, which combines the features of a suspicious transaction report and a CRF, and the duty of reporting suspicious transactions will apply to wire transfers, as well as currency transactions.[16]

When banks began regularly to report large currency transactions, money launderers responded by dividing large deposits into several deposits of under $10,000. A number of messengers are often used to make repeated deposits in several branches of the same bank or in several banks. In legal terms, this is "structuring" a deposit; on the street it is called "smurfing," a name derived from superactive characters in an animated cartoon. Structuring of deposits is itself now a crime.[17]

Money could be smurfed into banks by cash deposits through automated teller machines (ATMs), and in many cases could be withdrawn through an ATM in another country. This would avoid the hazard of facing a teller with a duffel bag full of cash. However, physical limitations on ATM deposits (stacks of bills will not go through the deposit slot) and monetary limitations on withdrawals (usually $300 to $500 a day) make this kind of international money laundering impractical for most criminal organizations.

Strong anti-money-laundering policies, including criminal referral and suspicious transaction reporting, impose costs on banks and may require them to assume a quasi-governmental role in taking on some of the duties of law enforcement. U.S. banks have developed a good track record in cooperating with law enforcement. They have in the last decade put in place policies and procedures, generally described under the rubric "know your customer," which are extolled by many bankers and law enforcement agencies. The Department of the Treasury is expected to issue formal "know-your-customer" rules in late 1995.

Some people outside of and even within the banking industry are, however, more skeptical, pointing out that such policies are not a complete solution. As criminals become more familiar with traditional customer identification procedures used by banks, they adopt new strategies or go back to reliance on old strategies such as smuggling cash across the borders and into foreign banks, from where it may be wired back into U.S. banks.[18]

## LAYERING: STRATEGIES FOR HIDING DIRTY MONEY

Money is still often smuggled out of (or into) the United States in the form of currency, but law enforcement agencies expend great resources trying to stop criminals from physically smuggling their cash profits across national borders, only to have the money flow without hindrance through electronic communication systems to countries where bank accounts are protected by secrecy laws.

By 1989, an American Bankers Association Task Force, while maintaining that stopping the placement of dirty cash through the bank teller's window is the top priority, nevertheless acknowl-

---

[15] CRFs have been required since 1989 under 12 CFR 21.11.

[16] Banks will not, however, be required to monitor wire transfers, many of which pass through the bank on automated systems (as will be explained in chapter 2), but merely to report those which do come to their attention and attract suspicion.

[17] Smurfers today are typically only peripherally involved in the drug trade, earning usually 1 percent of the funds they are able to deposit in banks. They may be, for example, day laborers, janitors, or hotel maids seeking to supplement meager incomes.

[18] "Stop the Smurfs," *ABA Banking Journal*, March 1992, p. 92.

edged that "Wire transactions, which are essentially unregulated, have emerged as the primary method by which high-volume launderers ply their trade."[19]

Suspect wire transfers are effectively hidden by the huge volume of legitimate transfers. There are about 700,000 wire transfers a day, of which perhaps from 0.05 percent to 0.1 percent represent money laundering (see chapter 4). The $300 million (or less) that is estimated to be laundered every day is dwarfed by the more than $2 trillion that is transferred by wire on an average day. Most criminal transfers are on their face indistinguishable from legitimate transactions.

Bank-to-bank transfers of aggregate funds for settlement or loans constitute about half of the total volume of wire transfers, but with the complicity of corrupted bank employees, these can also contain suspect money.[20] The primary reasons for bank-to-bank activity are Federal Reserve funds sales and returns, securities transfers and repurchase agreements, and settlement for cash letters. Many customer-initiated transactions are one-time only, and some are infrequent transfers spaced over a long period of time. The types of relationships and level of activity between U.S. banks differ greatly from those between banks in other countries, such as Canada and Australia, according to the American Bankers Association. The number of financial institutions, the constantly changing relationships and varying levels of activity make it difficult to identify suspicious activity.

One way of getting money into the banking system, more subtle and sophisticated than smurfing, is to provide a rationale or cover for its existence as cash. Money launderers may use a legitimate business as a front, or they may use "shell companies" (corporations that exist only on paper), often chartered in another country. In choosing a legitimate business to serve as a front, money launderers usually look for businesses with high cash sales and high turnover.[21] The size of the business is a consideration; a news stand or laundromat that deposits tens of thousands of dollars a day will soon attract suspicion. Once the illegal proceeds have been mixed with other money flows, they are extremely difficult to find. This is the step in money laundering described above as "layering," or passing the money through a number of transactions to confuse its trail.

International money launderers also use false invoicing. Greatly overpricing goods being imported into the United States can explain large amounts of money being wire transferred abroad. Researchers at Florida International University developed an analytical computer program to identify "irregularities" in government trade data—such as the pricing of the drug erythromycin at $1,694 a gram for imports, as compared with eight cents a gram for exports.[22] Their results indicate frequent use of inflated invoices. A federal grand jury in 1994 indicted five importers of medical devices on 50 counts of money launder-

---

[19] American Bankers Association (ABA) Task Force Recommendations, 1989, reprinted in the *Congressional Record*, May 8, 1989.

[20] Clifford Karchmer, "International Money Laundering: Analysis of Information on Successful Cases," October 1987, author's manuscript. Seymour Rosen of Citibank and Prof. Carl Felsenfeld of Fordham Law School agreed that approximately half of wire transfers are bank-to-bank transfers (i.e., not on behalf of a specific customer).

[21] Jewelers and gold merchants are also favored, since the buying and selling of gold is usually conducted in cash.

[22] Dr. Simon J. Pak and Dr. John S. Zdanowicz, Center for Banking and Financial Institutions, Florida International University. See Pak and Zdanowicz, "A Statistical Analysis of the U.S. Merchandise Trade Database and its Uses in Transfer Pricing Compliance and Enforcement," 1994 *Tax Management* (Bureau of National Affairs, Inc.), May 11, 1994.

ing involving wire transfers of $1.3 million (by wire) to Pakistan.[23]

Money laundering is associated with all categories of "crimes for profit" (as contrasted with "crimes of passion"), but to differing extents. Drug traffickers and other kinds of organized crime such as gambling and prostitution must struggle to get large volumes of small denomination bills to safety. The traditional American crime families, however, are thought to keep most of the money in the United States and to invest it in domestic assets; the South American cartels attempt to get the lion's share of the profits out of this country. "White collar" crimes (embezzlement, fraud, tax evasion) seldom require the placement of cash. Typically, in fraud cases, money extracted from the victims under false pretenses is in the form of their personal checks, which the perpetrator accumulates in one or more bank accounts and then wire transfers to an account in a country with strong bank secrecy laws. In real estate fraud, developers may take out huge loans, wire the money out of the country, and then declare bankruptcy. With terrorism and illegal arms trades, the intent may be to conceal the intended destination and use of funds as well as their origin.[24] There may be other significant differences in the characteristics of money laundering associated with different crimes, which further complicate attempts to define a profile or pattern by which money laundering can be recognized.

Law enforcement agents believe that organized crime lords and money launderers are highly flexible and agile at shifting among these various modes of money laundering, responding to changes and improvements in law enforcement initiatives. This is another factor that complicates efforts to lay out a "profile" of characteristics of money laundering that could be used to design other artificial-intelligence-based monitoring systems.

## THE GLOBAL UNDERGROUND ECONOMY

Electronic money laundering often requires the complicity of a foreign bank to serve as the immediate or final destination for illegal funds. Money launderers look for a country with a "dollar economy" or a place where U.S. dollars circulate freely—for example, Panama or Hong Kong. Especially favored are relatively or completely unregulated banks in the Caribbean nations that were formerly British colonies, for example, the Cayman Islands, a tiny British Crown Colony.[25] On the other hand, money launderers may choose a bank in a country such as Switzerland, Luxembourg, or Ireland, which have well-regulated banking industries but also offer tax advantages and bank secrecy laws that protect financial data.[26]

Legitimate companies also make much use of offshore banks, however, for a variety of reasons, most related to tax laws and regulatory structures, or what one economist has termed "national friction structures and distortions."[27] For example, U.S. banks send money to the Cayman Islands and other places to sidestep a Federal Reserve System (FRS) requirement that a percentage of deposits

---

[23] Press Release, U.S. Dept. of Justice, U.S. Attorney, Eastern District of Virginia, Nov. 3, 1994. See also, Milan Ruzickz, "Customs Targeting Fraudulent Trade Data," *Journal of Commerce*, Dec. 12, 1994, p. 1ff. In February 1995, however, a federal court convicted the defendants of structuring, filing false statements, and tax evasion but acquitted them of money laundering, because the government had not proven that the funds sent to Pakistan were proceeds of criminal activity. *Money Laundering Alert*, February 1995, p. 3.

[24] Money laundering is also said by the Department of the Treasury to be involved in illegal trafficking in nuclear materials and technology from the former USSR.

[25] A Crown Colony makes its own laws and regulations, although London appoints the governor and handles foreign policy. The Bank of England does not regulate banks in Crown Colonies.

[26] Norma Cohen, "Exploiting the Differences," *Financial Times*, April 30, 1993 (Survey Section, IV-1).

[27] Richard Anthony Jones, *Tax Havens and Offshore Finance: A Study of Transnational Economic Development* (New York: St. Martins Press, 1983), p. 1.

held in the United States be placed with the regional Federal Reserve Bank (FRB) each night in a reserve account that does not bear interest. Banks with a high volume of corporate accounts, reluctant to forego interest on this money (or to deprive their customers of interest) even overnight, may establish a branch overseas, "creating profit centers from which profits may be repatriated at the most suitable moment for tax minimization."[28] Both multinational corporations and individual investors may place money offshore for reasons related to cash management. The Eurodollar market is based in offshore banks.[29] As one economic geographer says, "Offshore finance is an essential and characteristic element of the contemporary world financial system."[30]

There are now at least 30 "international offshore financial centers." At present, the Cayman Islands alone boast 546 banks, including branches of 44 of the world's 50 largest banks, more than any cities except New York and London.[31] The Caymans also have about 600 mutual funds and 400 insurance companies (see box 1-4).

These uses of offshore banking centers are legal, and probably discourage any strong pressure by the U.S. government on other governments to restrain offshore banking. They also make it more difficult to distinguish transnational money laundering from legitimate commercial operations. Thus, Under Secretary of the Treasury Ron Noble speaks of international money laundering as "crime hidden in the details of legitimate commerce."[32]

Some banks in other countries may remain profitable, or may even be kept afloat, only because of the high volume of illicit money that enters or resides on their books. However, even the infamous Bank of Commerce and Credit International (BCCI), while it was deeply engaged in money laundering, was a legitimate and profitable bank in some of the countries in which it operated.

Complicity in money laundering has now become extremely risky for U.S. banks and bankers. Bankers may be jailed if convicted of complicity. The Department of the Treasury has the authority to levy monetary penalties for failure to comply with anti-money-laundering laws, and regulators are required to commence a proceeding to revoke the charter of a financial institution convicted of a BSA crime. Regulators do not wish to revoke bank charters except in extreme circumstances, since this would harm stockholders, hence there is sometimes reluctance to prosecute a banker. In fact, no bank charter has been revoked on the basis of BSA violations, but few U.S. banks are willing to take these risks except perhaps some nearing insolvency or owned or controlled by criminal organizations.

Some law enforcement officers argue that some foreign banks operating in the United States "lack a strong compliance ethic," because their home country traditions and culture emphasize bank secrecy. Overseas branches or offices of U.S. banks may also be a problem; the Office of the Comptroller of the Currency, which regulates national banks in the United States, can examine records of

---

[28] Susan Roberts, "Fictitious Capital, Fictitious Spaces: the Geography of Offshore Financial Flows," in Stuart Carbridge, Nigel Thrift, and Ron Martin, eds., *Money, Power, and Space* (Oxford, U.K.: Blackwell, 1994), pp. 91-115.

[29] Eurodollars are U.S. currency circulating outside of the United States, originally as a result of U.S. foreign aid after World War II and later as a result of chronic trade imbalances. (See box 1-4). In the 1960s, because of U.S. banking law and regulations (Regulation Q and the Interest Equalization Tax of 1963, for example), trading in Eurodollars abruptly moved from New York to London and offshore financial centers. See Susan Roberts, *op. cit.*, footnote 28.

[30] Susan Roberts, *op. cit.*, footnote 28, p. 111.

[31] "Cayman Islands," *Euromoney*, October 1994, pp. 40-46; Michael Schachner, "Big Spurt of New Captives for Cayman," *Business Insurance*, April 18, 1994, pp. 64-47; Chris Narborough, "Regulating Cayman Islands Mutual Funds," *International Financial Law Review*, August 1993, pp. 32-33; "Cayman Islands," *Euromoney*, May 1992, pp. 25-35; "Cayman Islands," *International Financial Law Review*, September 1992, pp. 14-20;

[32] FinCEN, *Year End Review 1994*, p. 5.

their foreign branches only with the permission of the host country. Countries with strong bank secrecy laws, including France, Germany, and Italy, do not give access to U.S. examiners.

Most of the knowledge that U.S. law enforcement agencies have about international money laundering and the criminal organizations that use it, is drawn from experience with western hemisphere drug trafficking.[33] Less is known about the heroin trafficking industry, especially that based in Southeast Asia, and the flow of money associated with it. In 1984, a Department of the Treasury analysis found that a large increase in small-denomination U.S. currency repatriated from Hong Kong to the United States appeared to parallel the increase in Southeast Asian heroin marketed in the United States. In the early 1980s, a National Intelligence Council document is said to have reported that ". . . the lion's share of heroin money probably is handled within Asia by the Chinese underground banking system."[34]

The explosion of organized crime in Russia, other former members of the USSR, and Eastern European nations also enormously increases opportunities for international money laundering. In 1994, General Mikhail Yegorov, head of the Organized Crime Control Department of Russia's Ministry of Internal Affairs, told a group of U.S. Senators that first on his list of professional concerns was "financial operations involving laundering of money [and] the penetration of these criminals groups into the economy of our country.[35] It was said at that time that nearly one quarter of the banks in Moscow are controlled by organized crime groups.[36]

## PROFESSIONALIZING MONEY LAUNDERING

Money launderers are increasingly sophisticated in manipulating financial systems and instruments. Professionals who have become white col-

---

[33] The Sicilian Mafia launder the proceeds of their own organized crime activities, often by commingling with the proceeds of Mafia-owned legitimate businesses; they are said to act also as money launderers for other criminal organizations or as brokers for independent money launderers. Jamieson, A., "Recent Narcotics and Mafia Research," *Studies in Conflict and Terrorism,* vol. 15, No. 1, January-March 1992, pp. 39-51. See also Mark Richard, Dep. Asst. Attorney General, Criminal Division, Dept. of Justice, in *Federal Government's Response to Money Laundering Hearings*, before the Committee on Banking, Finance, and Urban Affairs, U.S. House of Representatives, 103d Cong., 1st Sess., May 25-26, 1994. Greg Meacham, former chief of the Money Laundering Unit of the FBI, believes that because the American Mafia is a domestic organization very little of their drug profits go overseas, and they are not heavily involved with international money laundering. (Interview, March 14, 1992). Other experts point out, however, that since the U.S. government began aggressively pursuing the seizure of illegal assets, the American Mafia has had ample reason to seek shelter for its profits overseas.

[34] This document "reached the open literature in 1986" according to William L. Cassidy, in "Fei-Ch'ien—Flying Money: A Study of Chinese Underground Banking," annotated text of address before the 12th annual international Asian Organized Crime Conference," Fort Lauderdale, Fla., June 26, 1990. Cassidy cites James Mills, *The Underground Empire: Where Crime and Governments Embrace* (New York: Doubleday and Co., 1986). Mills in turn cites "a National Intelligence Council document prepared in the summer of 1983." Cassidy says that there are today gold shops and foreign currency dealers in Los Angeles, Hong Kong, and Bangkok, for example, "that facilitate money transfers in support of the narcotics trade" using mechanisms developed hundreds of years ago in China as a means of avoiding the necessity of carrying valuables over long distance at a risk of highway robberies and repressive tax measures by the Ching dynasty. These methods depended on indirect transactions, "chits," and a primitive kind of travelers checks. The same methods were developed by Jewish merchants in the Silk Trade in medieval times. (Howard Fast, *The Jews: the Story of a People* (New York: Dial Press, 1968). The ancient Chinese banking methods have been brought up to date with the use of computers, modems, public-key encryption for communication between money handlers in China and the United States. (William L. Cassidy, "The Impact of New Technologies on South East Asian Underground Banking," International Association of Asian Crime Investigations, 1993).

[35] U.S. Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, Hearings, *International Organized Crime and its Impact on the United States,* May 25, 1994, p. 37.

[36] *Ibid.,* p. 2.

## BOX 1-4: Expatriate Money

By some estimates, up to two-thirds of the nearly $380 billion of U.S. currency in circulation in 1994 was either overseas or "in the underground economy" and unaccounted for. Of all U.S. $100 bills, 69 percent are said to be overseas.[1] U.S. Customs officers report that about 60 percent of all new U.S. bank notes are going to Eastern Europe and the former USSR; many people in these countries keep all of their savings in U.S. currency, believing in its integrity and stability. In Panama and Liberia, U.S. dollars are the primary currency.

U.S. currency is carried overseas by travelers and spent there. It is sent overseas in regular large shipments by money center banks, to foreign financial institutions or to governments; or it is sent by other U.S. banks and businesses as a service to their customers overseas. As proceeds from criminal activities, it may be smuggled out of the United States. Foreign financial institutions commonly return only worn or damaged U.S. currency, or—less often-surplus bills not expected to be needed.

The Information just cited applies to currency. But about one-sixth of "Ml ," which includes all kinds of demand deposits and travelers checks as well as currency, is thought by some observers to be outside of the United States. This is about $2 trillion. Transactions between large multinational corporations (regardless of their country of origin) are usually conducted in these "Eurodollars," especially trade in commodities such as oil, coffee, sugar, gold, and silver.[2]

[1] Frederick B Verinder, Deputy Assistant Director, Criminal Investigations Division, Federal Bureau of Investigation, in Hearings on *federal Government's Response to Money Laundering Hearings,* before the Committee on Banking, Finance, and Urban Affairs, House of Representatives, 103rd Congress, 1st Session, May 25-26, 1993.

[2] Joel Kurtzman, *The Death of Money (New* York: Simon & Shuster, 1993), pp. 85-95.

SOURCE Office of Technology Assessment, 1995.

lar criminals provide "the link between the underworld and limitless commercial and financial opportunities in the legitimate sector" of the economy.[37] These are often lawyers or accountants.

In the large drug trafficking operations or cartels of South and Central America, there is generally an effective separation between the part of the organization actively involved in drugs distribution and that which provides money laundering and reinvestment.[38] In most cases, the actual money launderers are not cartel employees but contractors, often serving several drug trafficking organizations. Colombian cocaine cartels are said currently to pay contractors a 20 percent fee for money laundering; the contractors give the cartel a certified check for 80 percent of the dirty cash, up

[37] Clifford Clifford and Douglas Ruch, "State and Local Money Laundering Control Strategies," *National Institutes of Justice Research in Brief,* October 1992. OTA was told by law enforcement personnel and also by a convicted money launderer (who himself fit this profile) that money launderers (except for "smurfers" and smugglers) were typically well-educated professionals. However, an analysis by the U.S. Sentencing Commission of the 943 persons convicted of money laundering in 1992 showed that 17.7 percent were college graduates and another 25.9 percent had some college training. ("Convicted Launderers Fit White-Collar Profile," *Money Laundering Alert,* December 1993, p. 2.) It maybe that those with most professional training are more successful and less likely to be caught or convicted.

[38] FinCEN, *An Assessment of Narcotics-Related Money Laundering.* FinCEN Reference Series, Redacted Version, July 1992. The lower level drug distributors must launder only their own salaries or commissions, and are likely to do this either through depositing the money into local banks or smuggling money across a land border.

front, and themselves assume the risk of cleaning it.[39] The cartels operate much like large multinational corporations, and their money laundering operations are becoming global in scope. Three Colombian drug kingpins—Pablo Escobar, Jorge Ochoa, and Jose Gacha—were in *Forbes'* list of the world's billionaires in 1988.[40]

Financial institutions and their wire transfer systems provide the battlefield for the struggle to control money laundering. The internationalization of financial services has created a highway for the movement of the profits of international crime.[41] Much of the money from drug trafficking is thought to return to this country after being laundered, either to pay wages, bribes, commissions, and other expenses, or for investment in legitimate businesses, real estate, or the securities market.

The great importance of this reverse flow to criminal organizations has sometimes been overlooked in law enforcement detection strategies. These strategies tend to focus on the flow of illegal profits out of the United States rather than reinvestment in the United States. The two-way flow, in theory, offers a double opportunity for detection and seizure, but the illegality of funds is far more difficult to detect and document on the return trip. Law enforcement agencies are becoming more aware of this problem, and in early 1995, the New York Stock Exchange for the first time took action against a member for failure to monitor the receipt of suspicious cash, money orders, and wire transfers.[42]

Securities houses are obligated by the Annunzio Wylie Anti-Money Laundering Act of 1992 to report large currency transactions and use of foreign bank accounts by American customers. Brokerage houses may be prosecuted for participating in money laundering, and customers' funds being held by the brokerages as collateral (i.e., margin) may be seized in forfeiture actions. Few CTRs are in fact filed, because it is unusual for securities transactions to be settled in cash and few securities firms will accept cash from a customer. The 1992 act authorized the Department of the Treasury to write rules requiring all nonbank financial institutions such as securities houses to have anti-money-laundering compliance programs, but these rules have not yet been issued. They are expected to require broker dealers to file suspicious transaction reports,[43] including "the use of wire transfers and other complex transactions or devices by the firms' clients to hide the illicit sources

---

[39] Interview with Greg Meacham, Chief of the Government Fraud Unit, Federal Bureau of Investigations, March 14, 1994. The Colombian criminal organizations known as the Medelin Cartel and the Cali Cartel have dominated global trade in cocaine. The Medellin cartel leader, Pablo Escobar, was killed by Colombian law enforcement authorities on Dec. 2, 1993, after a 17 month manhunt; this is reported to have "effectively dealt the *coup de grace* to the organization." (U.S. Dept. of State, *International Narcotics Control Strategy Report,* April 1994, p. 1.)

[40] By 1993, however, only Escobar—estimated worth $1 billion—was on the Forbes list, and the others were in jail; by the time of the 1994 list, Escobar had been killed. For more about these men, see Guy Gugliotta and Jeff Leen, *Kings of Cocaine: Inside the Medellin Cartel* (New York: Simon and Shuster, 1989).

[41] Some law enforcement experts suggest that more than half of the dollars generated by the sale of illegal drugs in the United States flow out to South American drug cartels.

[42] The New York Stock Exchange (NYSE), a self-regulatory organization, fined the Adler Coleman Clearing Corp. $75,000 for failing to have in place procedures required by Securities and Exchange Commission (SEC) regulations. A year earlier the NYSE disciplined another member found to have commingled a large amount of cash from a customer with money of his own without reporting it, although his firm's policy was to ask clients who wanted to pay with cash to exchange it for a cashier's check. *Money Laundering Alert,* February 1995, p. 5.

[43] About 300 suspicious transaction reports per year are filed by securities houses, generally by checking a box on a CTR. As noted, cash transactions are rare in the industry and therefore may usually be regarded as suspicious. (Alexandria Peers, "Brokers Probed in Laundering of Drug Money," *The Wall Street Journal,* Sept. 21, 1994, p. A3).

of their funds."[44] They will also probably provide a "safe harbor" against customer suits for such reporting. At present, since no tax withholding is necessary for foreign investors, such investors' social security numbers need not be recorded and their securities can be registered under the name of a lawyer or a fictitious company.

Several kinds of specialized bank accounts, in conjunction with wire transfer services, invite misuse by sophisticated professional money launderers. "Threshold accounts" are programmed so that when the funds in the account reach a predesignated level, they are automatically wired to a foreign account. The foreign account could be a "cupo account," which registered U.S. export/import companies maintain in a foreign country; cupo accounts are allowed to receive a certain quota ("cupo") of U.S. dollars. The export/import company may itself need only a portion of this dollar allowance, letting it be known that the account can also—for a fee—serve as a haven for drug-trafficking profits wired into the account from the United States.[45]

Foreign firms may establish master correspondent accounts in a U.S. bank as "payable-through accounts." They then give their foreign customers signature authority to use the account to transact business in the United States, including the use of wire transfer services and the right to make cash deposits and withdrawals. The foreign customers are generally known to the U.S. bank only as a name, thus subverting the "know your customer" policy. Payable-through accounts are thought to have become much more common as foreign banks found it harder to get approval to operate in the United States following the BCCI scandal. However, no one knows how many such accounts are held by foreign banks, or how many of their customers have been allowed to use the account, for a fee. Some reports say a single account may be used by thousands of individuals and by other foreign banks.[46] The FRS and the Office of the Comptroller of the Currency (OCC) in March 1995 issued new guidelines, asking banks to tighten rules governing the use of the accounts and to insist on having information about every authorized user.

## NONBANK MONEY TRANSMITTERS

Banks have been the chief focus of attempts to control the use of wire transfers for money laundering, but there are also an estimated 200,000 nonbank money transmitters. These are businesses that specialize in transferring money for customers, usually individuals; most also sell money orders and travelers checks. They range from large national enterprises like Western Union and Interpayment Services[47] to small neighborhood businesses. The latter may specialize in services such as sending the wages of recent immigrants back to their families at home. In many cultures, people have always relied on informal, personal financial services, often provided by a wealthier neighbor or "patron." The use of small nonbank money transmitters perpetuates this tradition. Their activities often have a narrow geographical or ethnic focus. This is the segment

---

[44] Quoted from a memorandum from Branden Becker, Director of SEC's Division of Market Regulation, to Arthur Levitt, chairman of the SEC. Oct. 28, 1994, providing a response to questions posed on Sept. 21, 1994, by Rep. Edward Markey, then chairman of the Subcommittee on Telecommunications and Finance of the House Committee on Energy and Commerce. Mr. Markey asked about the responsibilities and activities of the SEC with respect to enforcement of anti-money laundering laws. His questions were prompted by an article appearing that day in *The Wall Street Journal* (Alexandria Peers, "Brokers Probed in Laundering of Drug Money," p. A3) reporting that major brokerage houses were being investigated for violations of anti-money-laundering laws. These allegations were denied by the Office of the U.S. Attorney for the Southern District of New York, according to a later article in *The American Banker* (Shannon Henry, "U.S. Denies a Report It's Probing Brokerages for Money Laundering," Oct. 6, 1994, p. 9).

[45] Mike Rosenberg, FinCEN, "Wire Transfer Presentation."

[46] "Finding Laundering Perils, Fed Cracks Down on 'PTAs'," *Money Laundering Alert,* March 1995, p. 1.

[47] Interpayment Services is the company that sells American Express Travelers Checks.

of the industry that is most often suspected of involvement in money laundering, but large nationwide firms have also been used by launderers.[48]

Check cashers and sellers of money orders provide necessary services for people who do not have bank accounts and neighborhoods that have been ignored or disdained by banks. The problem is that check cashing services may receive illegally earned currency and use it to cash legitimate checks for their customers, thus avoiding CTRs; or they can structure transmittals by issuing multiple travelers' checks and money orders for less than $10,000 each.

A task force appointed by the State of Florida to study the money transmitter industry concluded that it is increasingly being used by money launderers, but emphasized the value of the industry. Money transmitters "play a vital role in facilitating international trade and both foreign and domestic tourism," and the economies of many small countries would be seriously damaged without remittances from immigrants to the United States.[49]

Currency exchange booths (casas de cambio), check cashing services, and giro houses (neighborhood money transmitters) are usually used by money launderers on a relatively small, "retail" scale. They are reportedly used by drug cartels mostly for internal (intracartel) business such as employee payments, while the big profits flow through banks.[50]

A casa de cambio changes currency for travelers at a border, or can exchange currency for "bearer" monetary instruments that are readily fungible. In Colombia, for example, U.S. money orders are "as negotiable as cash," according to U.S. Customs agents.[51] A giro house can simply deposit the wages of an Honduran immigrant, for example, in its bank in Houston (aggregating it with other funds collected that day), and fax its agent in Honduras instructions to withdraw the same amount—less a substantial fee—from the giro house's disbursement account in an Honduras bank and turn it over to the immigrant's family. Alternatively, the giro may instruct its Houston bank to wire transfer money to an Honduran bank for disbursement to the family. The giro house—although legally required to file a CTR if the funds amount to more than $10,000—has ample opportunity to launder money by aggregating funds in its account at either end and by concealing the real identity of the sender and recipient. In any currency transaction over $10,000, both the money transmitter and its commercial bank should file a CTR covering that transaction, but this often does not happen. Some state law enforcement officials argue that most giro houses exist only to serve the

---

[48] On June 2, 1994, two private bankers working as agents for American Express Bank International were convicted of 11 counts of money laundering, four counts of deceiving Federal Reserve examiners by false representation, and two counts of bank fraud. (Note that American Express Bank International, a part of American Express, is not technically a money transmitter since it no longer is the seller of the travelers checks.) For a customer identified as a gasoline station attendant in Mexico, they had formed companies, opened bank accounts in Switzerland and the Cayman Islands, and sent and received "countless wire transfers of seven figures." The customer was in fact a money launderer for major Mexican drug trafficking operations. The American Express officials had falsified records about the customer in order to make them appear to conform to the bank's "know your customer policy." "Bank's Know Your Customer Policy Helps Sink its Officers," *Money Laundering Alert*, July 1994, p. 3. The two individuals were sentenced to terms of 10 years and 42 months, respectively. American Express Bank International was not criminally charged but entered into a settlement agreement, which required the company to pay $35.2 million, in order to avoid a civil suit and separate forfeiture action. "Am Ex Bank Unit Pays $35 million in Laundering Case," *Money Laundering Alert*, December 1994.

[49] State of Florida, *Final Report* of the Comptroller Gerald Lewis Money Transmitter Task Force, October 1994.

[50] However, a Los Angeles cocaine ring owned a check cashing service through which it laundered $4 million per month. (U.S. Dept. of State, *International Narcotics Control Strategy Report*, April 1994, p. 480).

[51] Thomas M. Loreto, Special Agent, U.S. Customs Service in New York City, in meeting with OTA staff, Nov. 14, 1994.

money laundering needs of drug traffickers, because the legitimate income generated by a giro would not be sufficient to sustain the operation.[52]

Forty-two states regulate check cashing and sale of money orders through licensing and bonding requirements. Only California and New York have separate statutory provisions regarding their funds transfer activities.[53] The Money Laundering Suppression Act of 1994 (signed September 23, 1994) requires all money transmitters to register with the U.S. Department of the Treasury,[54] and expresses the "sense of Congress" that states should enact uniform laws regulating money transmitters.[55] Although the money transmitters are classified as financial institutions, they are not depository institutions and therefore operate through accounts with commercial banks. In terms of wire transfers, the neighborhood giro houses are merely another link in the chain from originator to bank to wire transfer system to another bank (or banks) to the final beneficiary. Their intermediation can further obscure the trail of illegal money, as they lump together the funds of many senders and recipients in making their own deposits and transfers. A bank may not recognize that one of its accounts is servicing a money transmitter.[56]

New wire transfer regulations, to be discussed in the following chapter, will regulate recordkeeping by money transmitters as well as other kinds of financial institutions. Until these regulations, neighborhood money transmitters have necessarily created records for their own use, but these were usually limited to the amount of the transfer, the identity of the sender, and the name and location of the intended recipient.

There was usually no computerized record or database that could easily be searched by law enforcement officials, even with a search warrant.[57]

## THE OUTLOOK

Neither voluntary "know-your-customer" policies nor cash reporting requirements have yet succeeded in blocking the access of money launderers to the legitimacy and convenience afforded by bank accounts and access to wire transfer services. Nor is it expected that new know-your-customer or reporting regulations will solve the problems. Such regulations may become even more ineffective in the future for several reasons:

- the full-scale automation of wire transfer services, with more and more users having online access, and correspondingly less human intervention or monitoring;
- the tremendous growth in the volume and scale of international and multinational trade and business transactions, which obscures the parallel growth of illegal international operations,

---

[52] Interview with Michael P. Hodge, project director, and Thomas R. Judd, special counsel, Criminal Justice Project, National Association of Attorneys General, Aug. 9, 1994. Hodge and Judd noted that many giros appear to be set up for the purpose of clearing a specific "stash house" by writing fake receipts, and often disappear six or eight months after they are licensed—to reappear in another location and under a different name.

[53] State of Florida, *op. cit.*, footnote 49.

[54] A new Internal Revenue Service form was shown to the industry in draft (Form 9742) in April 1995, and will soon be published for comment.

[55] The law applies to businesses that cash checks, exchange currencies, issue or redeem money orders and travelers' checks, and transmit or remit money. It makes operation without a state license (where states require such license) a federal crime.

[56] In June 1994, U.S. Customs Service agents arrested 14 "subagents" of Vigo Remittance Corp. for money laundering. They had repeatedly transmitted money for undercover men posing as drug dealers, falsifying accounts accordingly. The company, which operates through 500 independent subagents in 35 countries, is alleged to have "failed to utilize existing computerized internal controls. . . and turned a blind eye toward the detection and prevention of money laundering by their subagents." The subagents deposit or wire the money to the company's accounts before it is sent on to its final destination. "U.S. Charges 14 Agents of Money Transmitter," *Money Laundering Alert*, July 14, 1994, p. 3.

[57] Typically, one copy went to the sender, one to the money transmitter's "foreign correspondent" (the agent or business that made the actual payment to the recipient), and a third was retained.

and puts pressure on banks to automate all services and make them widely accessible;

- the interdependence of financial institutions and clearing mechanisms around the world, which together with the speed of wire transfer systems, increases systemic risk and further discourages any intervention that may slow or interrupt payment systems;
- growth in the number of correspondent relationships between U.S. and foreign banks, and increasing use of specialized bank accounts than can be accessed by customers of foreign correspondent banks;
- The development of money management services, foreign exchange trading, swaps and derivatives trading, and other financial services with characteristics that resemble those thought by law enforcers to be characteristic of money laundering, thereby providing cover for illegal money operations;
- immigration patterns encouraging the proliferation of nonbank money transmitters, widely dispersed and more difficult than banks to regulate and monitor; and
- the expected emergence of new modes of payment, such as digital cash.

The ability of law enforcers to delineate a "profile" that can be used to spot money laundering appears to be limited by the following factors:

- the willingness of launderers to shift rapidly among laundering strategies such as physical smuggling of cash, conversion to monetary instruments, reliance on wire transfers, and use of nonbank money transmitters;
- the wide range of covers for wire transfer transactions: shell corporations and front companies, false invoicing, etc.;
- the similarity of illicit operations and legitimate operations, especially in businesses with high cash turnover;
- the growing professionalism and expertise of white collar money launderers; and
- lack of knowledge of characteristics of non-drug-related money laundering, and of money laundering associated with drug trafficking outside of South America.

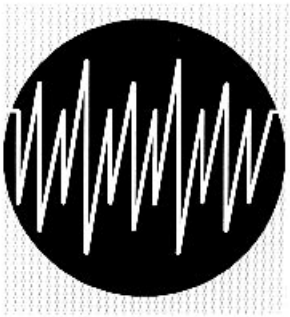
# The Mechanisms of Wire Transfer 2

In order to understand both the dynamics of international money laundering and some of the technological fixes that have been proposed for its control, it is necessary to understand the mechanisms that have developed for large-volume transfers of funds.

## MOVING MONEY: BOOK TRANSFERS AND ELECTRONIC TRANSFERS

The simplest funds transfers involve two accounts in the same bank. Here, money is moved from one account to another through "book transfers," or accounting changes by which funds are simultaneously debited from one account and credited to another. Each account may be either a customer account or the bank's own account.

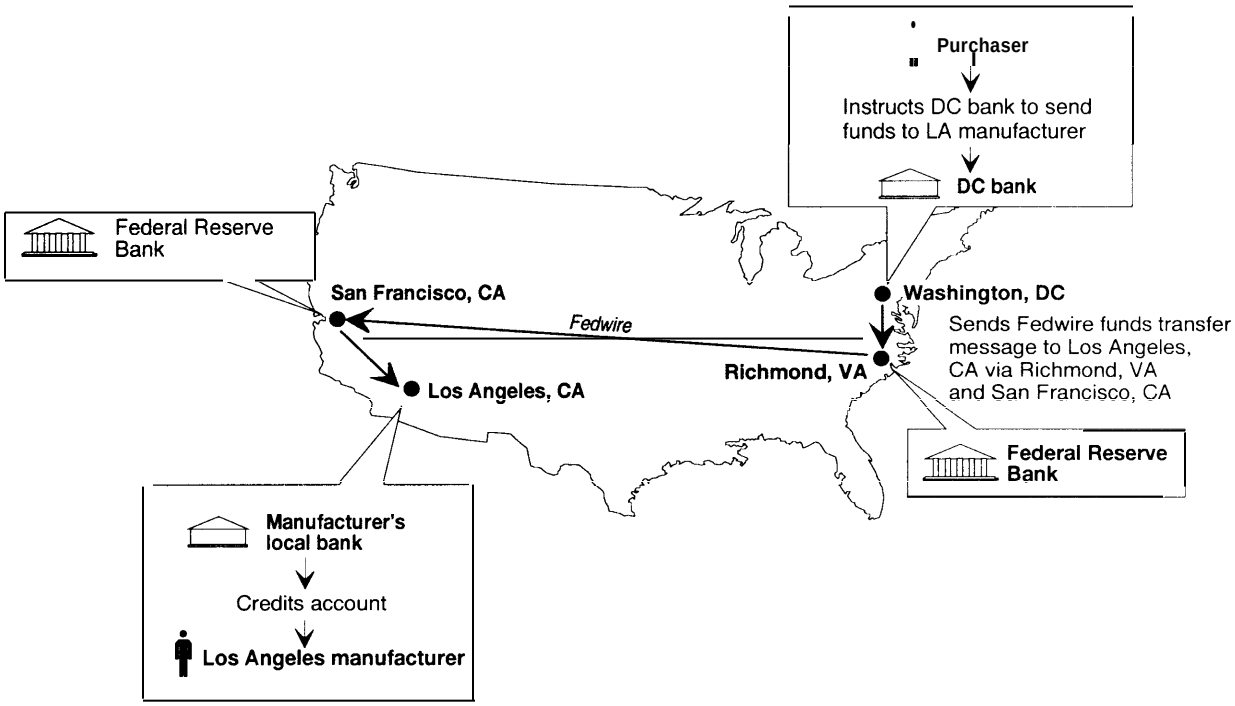
If the accounts at either end of a transaction are in different banks, a book transfer may still be accomplished directly if the two banks have a correspondent relationship. One bank maintains a "correspondent account" at the other bank for the purpose of settling transactions for itself or for its customers.[1] For example, Bank 1 will debit Customer A's account and credit its own account, and then send a verbal or electronic instruction (a payment order) to its correspondent bank, Bank 2. The payment order tells Bank 2 to debit the correspondent account of Bank 1 and pay the money to, or into the account of, Bank 2's customer B, the designated recipient.



If the two participants in a transaction use banks that do not have a correspondent relationship, the transfer will go through

[1] Correspondent relationships are usually, but not always, two-way relationships.

FIGURE 2-1: A Fedwire Transfer From Washington, DC to Los Angeles




SOURCE: Adapted from U S. Department of Treasury, Financial Crimes Enforcement Network, *Key Electronic Funds Transfer Systems Fedwire, CHIPS, SWIFT* Report OSA *92 CBO012* (Vienna, VA September 1992)

CHIPS or Fedwire from Bank 1 to the Federal Reserve Bank (FRB) in its District, which will move the funds from the account of Bank 1 into the account of Bank 2. If the two banks are not in the same Federal Reserve District, there is a further step in which the funds move by Fedwire from the Federal Reserve Bank in the sender's District to that in the receiver's district, and then to the bank representing the beneficiary. There are at least three legs to this transfer—sender to FRB to FRB to receiver (see figure 2-1).

## USES AND USERS OF WIRE TRANSFERS

Customers wishing to send money swiftly to another city or country may so instruct their banks in person or by telephone, fax, or telex. However, private (individual) wire transfer users are relatively few in number and account for only a small portion of wire transfers by number or by dollar volume. Most wire transfer users are large corporations sending large-dollar transfers. These corporate customers often have online access to the bank's wire transfer services, using software provided by the bank[2] (see box 2-1).

Legitimate businesses use wire transfers when sending very large sums or when the timeliness and certainty (irrevocability) of payments are of paramount importance-especially in foreign exchange transactions and securities trading. For routine payment for goods and services, they are

[2]In banks with large cash **management** departments, over 70 percent of wire transfers may be initiated through an automated link between the customer's microcomputer or mainframe and that in the bank's wire room. Philip C. Alwesh, "Addressing Risk in the Large-Dollar Payments System," *The Bankers Magazine,* July-August 1990, p. 16.

## BOX 2-1: The Legal Structure for Wire Transfers

Until 1991, there was no federal body of commercial law specifically governing wire transfers. The Federal Reserve Board's Regulation J established rules among Fedwire participants, and Fedwire and CHIPS were, and are, governed by state commercial law. The wire transfer systems differed in some regards about liabilities for failed transfers or requirements that wire transfer records be maintained by banks. Further safeguards were provided by contracts between banks.

Article 4A of the U.S. Uniform Commercial Code now provides the legal structure for wire transfers. It is a model law proposed for adoption by the states; it sets rules for, among other things, resolving disputes over responsibility for unauthorized or erroneous transfers and the effect of payment by wire transfer on other contractual obligations. [1] It was approved by the National Conference of Commissioners on Uniform State Laws in August, 1989, and subsequently by the American Law Institute in 1991.2 By the end of 1993, it had been adopted by 32 states, but it has still not been passed in all states. The Federal Reserve Board amended Regulation J to incorporate Article 4A and thus govern all Fedwire transfers, even in those states that have not adopted the model code.

While Article 4A was being developed in the United States, the United Nations Commission on International Trade Law (UNCITRAL) also drafted a model law to govern wire transfers. The two model laws were developed independently and with little reference to each other, but the drafting committees shared some members. The model laws are generally compatible, although the UNCITRAL law is much less specific.[3]

[1] Sarah Jane Hughes, "Policing Money Laundering Through Funds Transfers: A Critique of Regulation Under the Bank Secrecy Act," *Indiana Law Journal* 67, no. 2, Winter 1992.

[2] Carl Felsenfeld, "The Compatibility of the UNCITRAL Model Law on International Credit Transfer with Article 4A of the Uniform Commercial Code," *Commercial Law Annual* 1993. See also, Felsenfeld, "Strange Bedfellows for Electronic Funds Transfers: Proposed Article 4A of the Uniform Commercial Code and the UNCITRAL Model Law," *Alabama Law Review* 42, no, 2, Winter 1991.

[3] Felsenfeld, op. cit., footnote 2, 1993, Felsenfeld participated in drafting both model laws.

SOURCE: Office of Technology Assessment, 1995.

more likely to use checks or automated clearing house (ACH) payments.[3] Illegitimate businesses—including shell companies or front companies set up for money laundering—also seek the speed and irrevocability of funds transfers, in order to get their money beyond the grasp of law enforcement asset seizure. A critical task in any anti-money-laundering surveillance system would be to distinguish the spurious corporate wire senders from the legitimate businesses that overwhelmingly outnumber them.

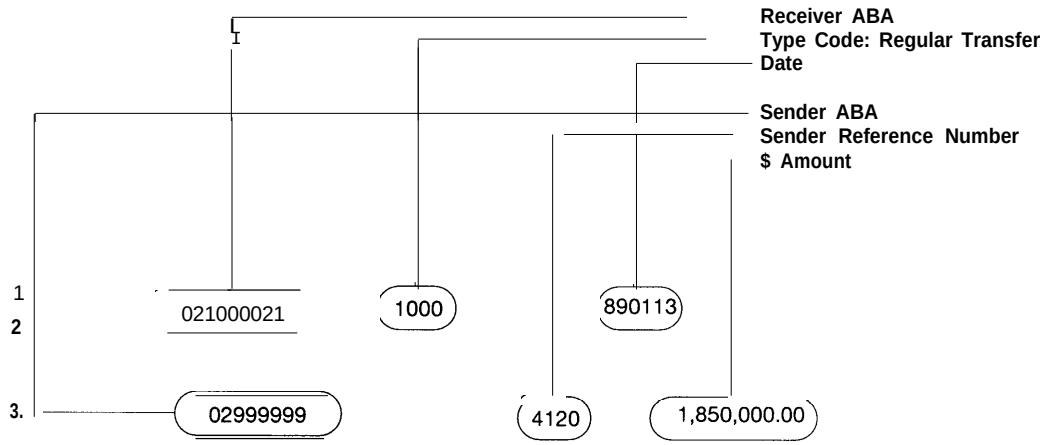
Banks in the United States engage in very active bank-to-bank transfer, including Federal Reserve funds movements, securities transfers, repurchase agreements, etc. The number of banks and the volume of bank-to-bank transfers are both much higher than in other countries.

U.S. banks chiefly use two wire transfer systems to carry out the exchanges with other banks. These are Fedwire, operated by the Federal Reserve Banks, and CHIPS (Clearing House for Interbank Payments System), operated by the New

[3] Scott E. Knudson, Jack K. Walton II, and Florence M. Young, "Business-to-Business Payments and the Role of Financial Electronic Data Interchange," *Federal Reserve Bulletin,* April 1994, pp. 269-278.

## FIGURE 2-2: Sample Fedwire Transfers Sent and Received

**Sample Fedwire Transfer Received by a Bank**

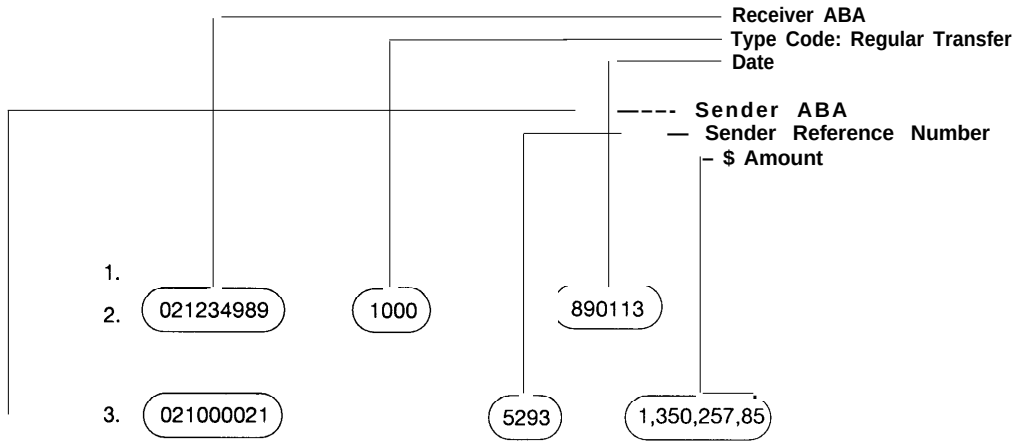



**Sender** *4.* **Hometown BUF/ ORG-Samuel S. Simpson, Sr.**

**Receiver** **5. Chase NYC/CTR/ BBK -University Bank BNE -Sanuel S. Simpson, Jr/K-9001 11**

**6. / PHN /232-333-5555 w-spending money**

**Sample Fedwire Transfer Sent by a Bank**




**SENDER** *4.* **Chase NYC/ ORG-For-tune 500 Corporation**

**RECEIVER 5. Anybank NYC/CTR/ BNF -Metropolitan Office Supplies/ AC-9899-12/PHN**

**6.W-INV155XA ~-Payment of Merchandise**

SOURCE: Financial Crimes Enforcement Network, "Key Electronic Funds Transfer System, Fedwire, CHIPS, SWIFT," September 1992, pp. 16-17

York Clearing House, an association of money center banks.[4] Approximately 11,700 banks have access to Fedwire; 115 large banks have direct access to CHIPS, some of which also act as intermediaries for middle-size and smaller banks.[5] Approximately 150 U.S. banks and 300 U.S. based subsidiaries of foreign banks are users of SWIFT (Society for Worldwide Interbank Financial Telecommunication), an international messaging system that carries instructions for wire transfers between pairs of correspondent banks.

## MONEY CENTER BANKS: GATEWAYS TO WIRE TRANSFER

About 15 or 20 banks in the United States are categorized as "money center" or world-class banks, and operate globally. Most international wire transfers moving to and from the United States pass through one of New York City's large money center banks in order to access CHIPS—these include Citibank, Chase Manhattan Bank N. A., Chemical Bank, Bank of New York, Marine Midland, Bankers Trust, Morgan Guaranty Trust, and the U.S. Trust Company. On an average business day, about 80,000 transactions (totaling nearly $500 billion) pass through the wire room at Citibank. Approximately 65,000 transactions (totaling about $400 billion) are processed through Chase Manhattan's money transfer operation. Most of the senders are other banks or nonbank financial institutions; very few are individuals.[6]

At Citibank, the funds transfer messages can arrive by telephone or telex, but for the most part they arrive over Citibank's private network of leased lines, connecting microprocessors in the offices of about a thousand customers. Citibank's "relationship managers" determine which customers have access to this network. About 70 percent of the arriving messages are directly shunted by Citibank's computers to another participating bank, directly or via CHIPS or Fedwire. The other 30 percent, however, must be "repaired"; that is, an operator must look at the message, correct the format, insert a routing address (a number for the next bank in the sequence), or make other changes before the computers can complete the transaction.[7]

Typical wire transfer messages are shown in figure 2-2 and figure 2-3. The information contained on a wire transfer message is generally limited to some or all of these items:

- the amount of the transfer,
- the date of the transfer,
- the name of the sender or "originator,"
- the routing number of the originating bank,
- the identity of the designated "beneficiary" or receiver of the funds, and
- the routing number of the recipient bank

Because one transfer may pass through several banks before reaching the beneficiary's bank, the separate payment orders necessary to the particu-

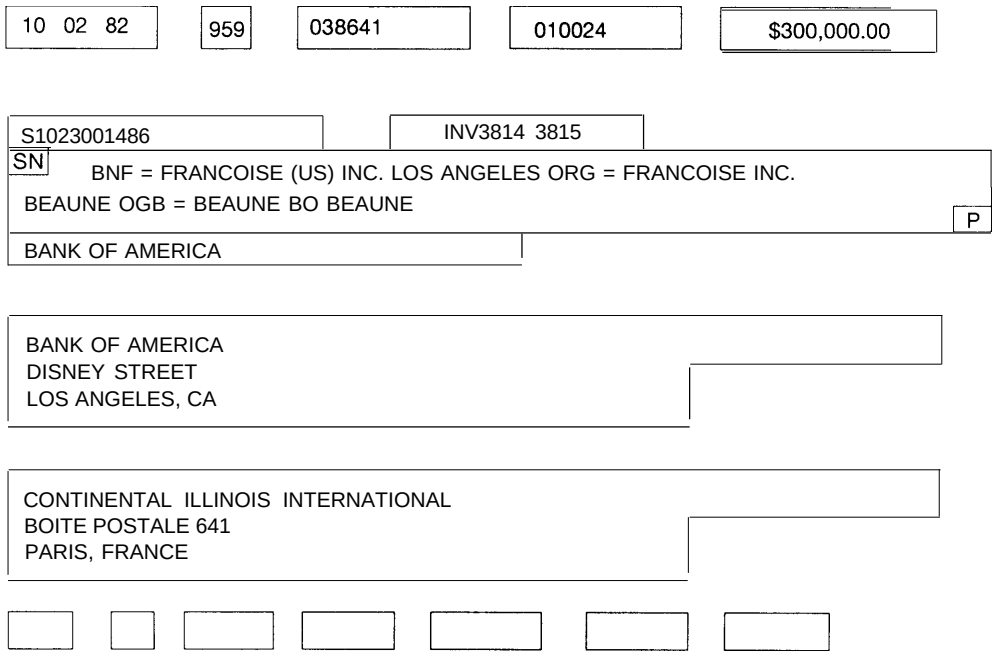
[4] In addition to FedWire, CHIPS, and SWIFT, there are four automated clearing house (ACH) networks that electronically facilitate the transfer of funds among domestic banks by sending instructions between correspondent banks to make book transfers. However, an automated clearing house is a batch processing message system, and is not considered a wire transfer system. (Federal Reserve System Regulation CC, 12 C.F.R. 229.2.) The ACHs are generally used for relatively small payments. Orders for payments through ACHs are usually bulk orders made several days in advance, for example an entire pay roll or a very large schedule of mortgage debits. Some corporate money management or "cash concentration" services use recipient-ordered debit transfers. Such arrangements could be utilized by money launderers masked by a front corporation, and there have been a few such cases. But because ACH payments are usually small, recurring, and submitted in bulk by well-established users, they are not an inviting mechanism for money launderers.

[5] There are, in the United States, more than 11, 700 commercial banks, but 15 percent of these banks hold three-quarters of all bank assets. The other 84 percent of US banks are "community banks," locally owned and operated, which have assets of a mean size of $42 million as compared with an average of $1.3 billion for the larger banks. (Information provided by the Independent Bankers Association of America.)

6 An individual wishing to wire funds wouId ordinarily be accommodated at a Citibank branch bank, so that this transfer would appear, in the Citibank wire room, as a bank-to-bank transfer.

[7] This adds a few extra cents to the cost to the client company but maybe cheaper than maintaining a larger or more expert staff within the company.

FIGURE 2-3: Hypothetical CHIPS Messages




SOURCE: Financial Crimes Enforcement Network, "Key Electronic Funds Transfer System, Fedwire, CHIPS, SWIFT, " September 1992, p 22

lar bank-to-bank transfer will contain different information. Often, as the payment order is reformatted for the next phase of the transfer, the bank will omit identification for earlier participants, such as the sender or intermediate banks. In the United States, the originator's account number has generally been dropped from subsequent payment orders to keep this information confidential. Some foreign banks, if requested, will omit the name of the originator and merely state "payable for our good customer."

Under new regulations made final in January 1995 and due to take effect in January 1996, identification of the originator and beneficiary is required and must travel with the message throughout the transfer.[8] Experts fear that foreign banks, which will not be bound by these regulations, will not include the identity of the originator because of bank secrecy laws in their country. They may be even more likely to use a generic, fictitious, or unidentifiable name for the originator, fearing broadened law enforcement access to the newly improved records.

Two other fields are sometimes filled in: bank-to-bank information and reference for beneficiary. These may carry potentially useful information for law enforcement, but they are generally in narrative, unstandardized format and therefore are not readily searchable.

## RETRIEVABILITY OF WIRE TRANSFER RECORDS

Most large banks have computer programs that can retrieve a specific wire transfer record, primarily as a service to their customers. New technology is making this easier and cheaper. For example, Chase Manhattan is now storing wire transfer records for two years on computer-searchable optical disks. Until recently, at Chase and at many

[8]60 Fed. Reg. 220 (Jan. 3, 1995), to be codified at 31 C.F.R. 103.

TABLE 2-1: NonCash Payments In the United States (

| Payment type | Volume of transactions (million) | % total volume of transactions | Value (trillions of $) | % total dollar value |
|---|---|---|---|---|
| Checks | 61,500.0 | 96.3 | $40.4 | 7.2 |
| Fedwire | 73.6 | 0.1 | 216.2 | 38.6 |
| CHIPS | 45.6 | 0.1 | 295.4 | 52.7 |
| ACH | 2,216.0 | 3.5 | 8.8 | 1.6 |
| Total | 63,835.2 | 100 | 560.8 | 100 |

NOTE For a variety of reasons, comparable data on SWIFT messages are not available. In 1994, there were 13,874,472 MT100s sent out of the United States At least that number were sent into the United States. A roughly comparable number of MT200s were sent in and out of the United States in 1994 The dollar volume represented by those messages is not available. Douglas Jeffrey, SWIFT, personal communication, May 22, 1995.
SOURCE" Off Ice of Technology Assessment, 1995

other banks, records were stored only on microfiche; these are difficult to retrieve except by the account number. Many middle-sized banks cannot electronically retrieve wire data more than a month old, and some small banks would have to search manually. However, their international money transfers normally go through one of the large money center banks.

Many large banks have now enhanced their recordkeeping systems in order to assure themselves and regulators that they are in full compliance with Bank Secrecy Act (BSA) regulations. Some have systems that monitor the wire transfer activity of certain accounts and generate periodic reports highlighting the consolidation of incoming wires followed by an outgoing wire transfer. These reports alert the bank's compliance department to review the activity against the bank's knowledge of the customer.

Most of these systems are designed to monitor customer accounts and do not take note of funds transfer services for nondepositors, or for which the bank only serves as an intermediary. At least one large bank, however, has a monitoring system designed to identify funds transfers sent by or to non-customers, or containing the instruction to "pay upon proper i.d.," when two or more transfers like this are sent or received within six months.[9]

## ELECTRONIC FUNDS TRANSFER SYSTEMS: DIGITAL PIPELINE FOR MONEY

Domestic and international funds transfers generally move through wire transfer systems. While Fedwire and CHIPS transfers together account for only about 0.1 percent of all payments in the United States, they carry more than 91 percent of all payments by dollar value (see table 2-l).

Wire transfers, like book transfers, become effective at the point when two accounts are respectively debited and credited. Transfers made over Fedwire are irrevocable and immediately effective, because the Federal Reserve Bank (FRB) guarantees the payment to the receiving bank as soon as the transfer message is sent. CHIPS payment messages are also irrevocable, but they are not finally settled until the end of the business day. At that time, payments and receipts for each CHIPS member bank are reconciled or netted. Should a participant be unable to settle at the end of day, its transactions for that day would all be "unwound" or undone, but in practice this unwinding is not allowed to happen. Banks whose payments have exceeded their receipts immediately send (by Fedwire) funds to cover their overdraft, from their account at the New York FRB to a CHIPS settlement account. CHIPS then sends

[9] Howard Cohen, "Dealing With Dirty $$$," *Bank Systems and Technology,* March 1990, p. 42.

TABLE 2-2: Fedwire Funds Transfer Volume

| | Transfers originated | | Annual growth rate | |
|---|---|---|---|---|
| Year | Volume (millions) | Value ($ trillion) | Volume (%) | Dollars (%) |
| 1980 | 26.2 | **47.9** | -- | |
| 1981 | 32.9 | **57.3** | 25.6% | 29.1 % |
| 1982 | 35.4 | **74.0** | 7.6 | 18,6 |
| 1983 | 38.0 | **87.8** | 7.3 | 18,6 |
| 1984 | 41,6 | **98.0** | 9.5 | 11.6 |
| 1985 | 45.1 | **109.1** | 8,4 | 11.3 |
| 1986 | 49.8 | **125.0** | 10,4 | 14,6 |
| 1687 | 53.3 | **142.3** | 7.0 | 13,8 |
| 1988 | 56.3 | **160.7** | 5.6 | 12.9 |
| 1989 | 59.9 | **182.6** | 6.4 | 13,6 |
| 1990 | 62.6 | **199.1** | 4.5 | 9.0 |
| 1991 | 65.0 | **192.3** | 3.8 | -3.4 |
| 1992 | 69.8 | **199.2** | 7,4 | 3.6 |
| 1993 | 71,2 | **207.6** | 2.0 | 4,2 |
| 1994 | 73.6 | **211,2** | 3.4 | 1.7 |

SOURCE: Federal Reserve Board of Governors

funds from its settlement account to those banks that ended the day with their receipts exceeding their payments. Records of all transactions are then sent to the participant banks on microfiche.

Another means of setting in motion international payments is SWIF. SWIFT is sometimes not considered an electronic funds transfer system as are Fedwire and CHIPS, but a specialized international cooperative communications service. About 150 U.S. banks and 300 U.S. subsidiaries of foreign banks participate in SWIFT, sending and receiving instructions about transfers to and from their correspondent banks around the world. Unlike CHIPS and Fedwire, SWIFT does not provide a mechanism for clearing and settling transactions. However, SWIFT messages are accepted as authoritative, and SWIFT meets the definition of a funds transfer system of the U.S. Commercial Code.[10] It will be treated here as a wire transfer system.

Fedwire, CHIPS, and SWIFT keep records of wire transfers, although there are differences in the way their records are stored and maintained.

## Fedwire

Fedwire, operated by the Federal Reserve System, began operations in 1918, originally using Morse code to send messages over leased telegraph lines. It now connects the 12 FRBs and 11,700 depository institutions within the United States. An average of over 293,000 transactions are carried over Fedwire daily, transferring a daily average of over $841.4 billion. The average amount of funds moved by one Fedwire transfer is nearly $3 million, and the cost of one transfer is about 50 cents (see tables 2-2 and 2-3).

More than half of the dollar volume in Fedwire transfers originates with the Federal Reserve Bank of New York on behalf of banks in its dis-

[10] U.C.C. Sec. NA- 105.

TABLE 2-3: 1994 Fedwire Funds Transfer Volume Statistics

| | Volume of transactions | Dollar value ($M) |
|---|---|---|
| Boston | 4,539,997 | $110,155,393 |
| New York | 25,911,720 | 124,045,888 |
| Philadelphia | 3,622,300 | 6,815,659 |
| Cleveland | 3,477,541 | 9,660,640 |
| Richmond | 3,525,621 | 6,508,227 |
| Atlanta | 4,814,030 | 6,502,163 |
| Chicago | 8,142,844 | 17,201,781 |
| St. Louis | 1,871,597 | 2,519,741 |
| Minneapolis | 1,783,930 | 2,769,423 |
| Kansas City | 3,330,098 | 5,261,331 |
| Dallas | 3,772,125 | 5,103,037 |
| San Francisco | 8,819,132 | 14,658,257 |
| Total | 73,610,935 | 211,201,540 |

SOURCE Federal Reserve Board of Governors

trict, because New York is the nation's financial center. Little is known about the relative importance of various Fedwire transfers, or who sends them.[11]

Fedwire transfers involve U.S. domestic transactions. However, the U.S. office of a foreign bank may be connected to Fedwire; money transferred to it may then be internally credited to the home country bank and hence to a customer account in that country. There are other ways of using Fedwire to effect a transaction that begins or ends outside of this country.

Over 99 percent of all transfers processed by Fedwire are entered by depository institutions "on line." The Federal Reserve monitors only the transfers of institutions in poor financial conditions to assure that they do not transfer more than they have in their accounts or their allowed daylight overdraft; and for most of these institutions, even this is done on an "ex post" basis only, not in real time. Most of the transfers are therefore not seen by anyone.

Fedwire processing was decentralized, occurring at each of the 12 regional FRBs until 1994, when processing for several FRBs was merged, resulting in a total of three processing sites. By the end of 1995, wire transfer records processing for eleven of the banks will be consolidated at a single site. It will then become possible to search at one time for records created (in 1995 or later) in any of the 11 banks. Eventually, processing for the Federal Reserve Bank of New York, which has by far the largest volume of traffic, will be merged with the rest.

Each of the FRBs has the capability of computerized scanning and retrieval of wire transfer records while they are online, for the first 180 days after they are created. Thereafter, they are maintained on microfiche (referred to as "the journal"), and manual searching is necessary) .12 The FRB

[11] One study showed that on one specific day, 38 percent were sent for purchase or redemption of securities, and another 20 percent were federal funds. The origins of the securities-related transfers were highly concentrated, in brokerage houses and a few large investors. ("A Study of Large-Dollar Payment Flows Through CHIPS and Fedwire," Federal Reserve Bank of New York, December 1987). Fedwire system managers disclaim any further knowledge.

[12] For a description of search procedures, see a Dept. of Justice Memorandum from Assistant Attorney General Jo Ann Harris, criminal Division, to all U.S. Attorneys, Jan. 13, 1994, on the topic of law enforcement access to Fedwire records.

computers can search for an exact match for up to 25 specific alphanumeric characters, so the sought record must be precisely identified.[13] Daily indices summarize the transactions of each bank (see table 2-4).

The Electronic Communications Privacy Act (ECPA) is considered to forbid access to electronic Fedwire (and CHIPS) records without a search warrant or, for records stored for more than 180 days, a subpoena.[14] Even with a search warrant or subpoena, it is generally necessary to provide to the Federal Reserve Bank all of the information needed to identify the record in the daily index.[15]

The Federal Reserve is now modifying the Fedwire funds transfer software format to provide a more comprehensive set of data elements, in order to "improve efficiency by reducing the need for manual intervention when processing and posting transfers," and to meet the requirements of new Treasury Department regulations concerning funds transfer records. The expansion will eliminate the need to truncate payment-related information from transfers received via CHIPS and SWIFT and then forwarded through Fedwire. The formatting should be fully implemented by the end of 1997.

## CHIPS

International dollar transfers usually move through CHIPS, operated by the New York Clearing House Association, whose members are 11 New York City money center banks.[16] There are 115 CHIPS participants representing 29 countries.[17] CHIPS is the mechanism used by very large banks to transfer and settle international and domestic business transactions conducted by these banks on behalf of themselves, their customers, and other nonmember banks[18] (see box 2-2). These transactions include, for example, commercial payments; loans; interest disbursements; Eurodollar placements; and foreign exchange sales and purchases, and swaps.

CHIPS now carries more than 95 percent of all international transfers that are denominated in dollars. It handles a daily average of 181,673 transactions amounting to about $1.18 trillion. On January 17, 1995, a record dollar volume was set amounting to $1.957 trillion; the record number of

[13] Up to 20 searches may be conducted simultaneously. The computer can thus be instructed to look for, for example, ten names or versions of one name, five addresses, and five bank account numbers. Searches take about 15 minutes for each day of records inspected. Searches are conducted after the close of a business day and can identify records created that day or during the prior 180 days; however, it may take up to a week to process the search request and schedule the search.

[14] Stored Wire and Electronic Communications and Transactional Records Access, Title II of ECPA, 18 U.S.C. 2701-2710.

[15] Federal Reserve System Press Release, Dec. 22, 1994.

[16] The New York Clearing House began in 1853, to improve the settlement process among member banks by centralizing the exchange of checks and other financial instruments. CHIPS was established in 1970 to eliminate the use of official checks for international transfer of dollars.

[17] From March 31, 1995, when one participant withdrew, until June 1, when another bank officially joined, there were 114 participants. CHIPS participants include domestic commercial banks, private banks, subsidiaries of domestic banks set up under the 1919 Edge Act to handle international business, and foreign banks, all of whom must have headquarters or branch offices in New York City in order to have access to CHIPS. About 70 percent of CHIPS participants are foreign banks.

[18] Of the 114 or 115 CHIPS participants, 18 are "settling members" and of these, eight have been approved to settle for the account of other participants in addition to themselves. At the end of the day CHIPS sends a balance report to each participant showing its net end-of-day position. Each settling member has 45 minutes to decline to settle for any participant for whom they are responsible (none has ever declined). The Clearing House then orders the Federal Reserve Bank of New York to open the settlement account; settling participants in a debit position then send funds by Fedwire to the settlement account; when these have been received, the Clearing House sends funds by Fedwire to the accounts of settling participants in a credit position; finally, the Clearing House notifies all participants that settlement is complete.

C C E DATE 89 RANSAC ON RECAP REPOR RUN D E 89 ME 9 P GE

RO: BUS NESS UNDS RANS ER ACCOUN PE D

| DR/CR Acct | Other Acct | Reference No. | Type | I M A D | TRCD | Fee Setting | Fee | a a Amt. | DR/CT |
|---|---|---|---|---|---|---|---|---|---|
| 0210-0002-1 | 0 11- 234-5 | 0004 | 1000 0113 G1233509 | 000004 01131451 | 00 | | | .40 | Debit |
| 0210-0002-1 | 0 11-2333-4 | 2000 | 1000 0113 F3123445 | 000006 0 131322 | 10011 | R1000000000 | .50 | 1,250,234.30 | Debit |
| 0210-0002-1 | 0222-3333-5 | 2452 | 1000 01 3 A 345987 | 000045 01131123 | 1001 | R1000000000 | .50 | ,250,445.42 | Debit |
| 0210-0002-1 | 0222-4444-5 | 4543 | 1000 0 3 C1234987 | 000034 0 31344 | 10011 | R1000000000 | .50 | 1,268,403.33 | Debit |
| 0210-0002-1 | 0111-1234-5 | 0059 | 1000 0113 17895670 | 000023 01131051 | 10011 | R1000000000 | .50 | 1,271,525.11 | Debit |
| 0210-0002- | 0 1-2333-4 | 0987 | 000 0 13 K1235644 | 000067 0113 531 | 100 1 | R1000000000 | .50 | 1,268,000.00 | Debit |
| 0210-0002-1 | 0222-3333-5 | 2349 | 1000 0113 A1365663 | 000234 01131451 | 100 1 | R1000000000 | .50 | 1,300,000.00 | Debit |
| 0210-0002-1 | 0222-4444-5 | 0987 | 1000 0113 B0C27 | 002344 01131322 | 10011 | R1000000000 | .50 | 1,300,000.00 | Debit |
| 0210-0002-1 | 0111-1234-5 | 5676 | 1000 0113 B4526783 | 005674 01131123 | 1001 | R1000000000 | .50 | 300,000.00 | Debit |
| 0210-0002-1 | 0111-2333-4 | 0834 | 1000 0113 B2344897 | 000345 0 131344 | 10011 | R1000000000 | .50 | ,300,000.00 | Debit |
| 0210-0002-1 | 0222-3333-5 | 2452 | 1000 0 3 B4523783 | 000052 0 131051 | 10011 | R1000000000 | .50 | 1,301,395.31 | Debit |
| 0210-0002-1 | 0222-4444-5 | 4543 | 000 0113 BXV23 | 000344 0113 531 | 0011 | R1000000000 | .50 | 1,303, 80.55 | Debit |
| 0210-0002-1 | 0101-1234-5 | 0059 | 000 0 13 B4526788 | 000223 01131451 | 100 1 | R1000000000 | .50 | 1,335,000.00 | Debit |
| 0210-0002-1 | 0101-2333-4 | 0987 | 1000 0113 B2334557 | 000245 01131322 | 100 1 | R1000000000 | .50 | 1,336,200.00 | Debit |
| 0210-0002-1 | 0202-4444-5 | 2349 | 1000 0113 B4523783 | 000456 01131123 | 10011 | R1000000000 | .50 | 1,341,803.05 | Debit |
| 0210-0002-1 | 0101-1234-5 | 0987 | 1000 0113 C1233387 | 000234 01131344 | 10011 | R1000000000 | .50 | 1,350.000.00 | Debit |
| 0210-0002-1 | 0101-2333-4 | 5676 | 000 13 17895634 | 001877 0 131051 | 10011 | R1000000000 | .50 | 1,350,0 3.00 | Debit |
| 0210-0002-1 | 0212-3498-9 | 4012 | 1000 0 3 B1234567 | 002032 01131237 | 100 1 | R1000000000 | .50 | 1,350,257.85 | Debit |
| 0210-0002-1 | 0984-5468-0 | 2452 | 1000 0113 A1365663 | 003145 01131451 | 10011 | R1000000000 | .50 | 1,390,066.78 | Debit |
| | | 4543 | 1000 0113 B2347897 | 002254 0113 322 | 100 1 | | | | |

KEY TO CODES:
DR/CR ACCT = bank account that is sending wire transfer.
OTHER ACCT = bank account that is receiving wire transfer.
REFERENCE NO = the sending or receiving bank's reference number fo the particular wire transfer.
TYPE = The type of transaction occuring through Fedwire.
IMAD = Input Message Accountability Data, various data regarding the particular Fedwire terminal through which the wire transfer proceeded ned not interpret.
TRCD = The code for the particular type of transaction.
FEE = The amount charged for the transaction.
Transaction AMT = The amount of money transferred through Fedwire.

SOURCE: Financial Crimes Enforcement Network (FinCEN), *Key Electronic Systems: dwire CHIPS, SWIFT* FinCEN Reference Series, Annex B-C, p.15.

## BOX 2-2: Examples of CHIPS Transactions

**1. Foreign and domestic trade services**

- British china manufacturer receives order for table settings from French retailer, to be paid for in U.S. dollars,
- British manufacturer notifies its Paris warehouse to fill order.
- Retailer acknowledges receipt and instructs Paris bank to pay British manufacturer in U.S. dollars.
- Paris bank advises its New York office to pay.
- Payment is sent via CHIPS from New York office of Paris bank, to New York office of British bank used by British manufacturer.
- New York office of British bank notifies its London office of receipt of payment,
- London bank credits china manufacturer's account.

2. **Foreign currency transactions**

- A U.S. manufacturer of airplanes fills a $45 million order for a jetliner from a carrier based in Rome; the carrier asks its bank to arrange payment,
- The Rome bank charges the airline's account for the lire equivalent, and arranges through the Rome branch of a U.S. bank to buy $45 million in U.S. dollars,
- The U.S. bank branch in Rome notifies its headquarters in New York to complete the foreign currency transaction, In New York, the U.S. bank delivers $45 million via CHIPS to the New York office of the Rome bank,
- The Rome bank in New York then pays $45 million to the U.S. airplane manufacturer,

3. **International loan syndications**

- A New Zealand telecommunications corporation needs a short-term loan of $50 million to purchase a computerized directory assistance system from a U.S. telecommunications company.
- It signs a loan agreement with its U.S. bank, which has agreed to put together a worldwide syndicate of 15 banks to make the loan.
- All 15 participating banks fund their share of the loans via CHIPS payments,
- The (U. S.) lead bank, through its New York headquarters, pays the money through CHIPS to the New York office of the borrower's New Zealand bank.
- The New Zealand bank (in New York) notifies its Auckland headquarters to credit the account of the New Zealand telecommunications company with $50 million, which then pays the U.S. company for the system it has bought.
- Over the life of the loan, the New Zealand corporation pays interest and principal via CHIPS to the lead bank in New York.
- The lead bank in turn disburses the appropriate shares of the repayments to the syndicate participants via CHIPS.

4. **Exchange of currencies**

- A Swiss entrepreneur locates office space to open a New York branch and needs $40,000 to make down payment; a Zurich bank is instructed to make payment.
- The Zurich bank orders its New York office to debit the bank's account and make payment of $40,000 to the New York realtor.
- The New York office of the Zurich bank makes payment through CHIPS to the realtor's bank, in New York,
- The realtor's bank credits the realtor's account and notifies the realtor that payment has been made by the Swiss entrepreneur.

SOURCE: The New York Clearing House Association, "Clearing House Interbank Payments System," 1995

transactions, 367, 142, was reached on February 21, 1995.[19] About 80 percent of CHIPS transfers are initiated by SWIFT messages instructing CHIPS participants to make a transfer on behalf of another bank that is not a CHIPS participant.

A CHIPS participant sends a payment message over leased lines to the CHIPS central computer, where it is checked and authenticated. The CHIPS computer then automatically records the debiting and crediting and sends a "receive" message to the receiving participant.[20] A net position is calculated for each participant at the end of the business day, and a final settlement is made.

CHIPS messages are required to carry only identification of the sending participant and the receiving participant (both CHIPS members), and the date and amount of the transaction. The sending and receiving participants may not be the originator's or the recipient's banks, but intermediaries—the large banks that transmit on behalf of nonparticipants. The CHIPS standard format includes data fields for identifying the originator's bank and the beneficiary's bank and other intermediary banks, but many CHIPS payment messages do not use these fields or put in only coded numbers identifying a general receiving or clearing bank account.

Tracing a transfer through CHIPS and linking it to a specific customer account is difficult but possible. All CHIPS transactions are kept on magnetic media for six months. Transactions since August 17, 1992, are being kept on optical disk; earlier records were maintained on microfiche for seven years. Finding a record was still possible if the date and the system sequence number assigned by the CHIPS computer were known, but it has generally been easier to work through the CHIPS participants.

## SWIFT

SWIFT, as already noted, is technically not a funds transfer system but a specialized communication system, owned by its member banks. Headquartered in Belgium, it was set up in 1973 and by March 1995 had 2,645 member banks in 124 countries, including 450 in the United States. It has over 4,700 users,[21] including securities brokers and dealers, stock exchanges, clearing systems, and other kinds of financial institutions.

Nearly 75 percent of SWIFT messages are payment instructions between banks, but SWIFT also carries messages regarding foreign exchange and money markets, securities, and trade financing.[22] It handled 518 million messages in 1994 (2.4 million daily average, and 2.5 million on the peak day); roughly 220,000 payment instruction messages a day are sent to or from the United States.

SWIFT messages are encrypted automatically by SWIFT's regional computer as they are received from a bank's input terminal. (Most banks also encrypt the message during that first leg.) The messages flow through the SWIFT system without any person seeing their unencrypted contents. An authentication algorithm guarantees the identify of the sender and receiver and reveals any alteration made illegally during transmission.

With SWIFT messages, the identity of the person or institution "on whose behalf" a bank is sending an instruction may or may not be specified.[23] To identify or trace a message requires the specific number identifying the input sequence or

---

[19] Data provided by CHIPS, March 7, 1995.

[20] It costs a participant between 13 cents and 40 cents to send a payment instruction through CHIPS, depending on whether the intended beneficiary's name and address must be entered into CHIPS database or is already on record with a full set of identifiers.

[21] Only the banks are shareowners in the cooperative, and hence voting members.

[22] *SWIFT Annual Report*, 1993.

[23] A SWIFT message includes, in code, a transaction reference number assigned by the sender, the date, amount of the transaction, the currency denominated, the sender's name and address, and the beneficiary's name and address. It may also include identification of the sender's bank and correspondent banks, the bank at which the beneficiary is to be paid, and the reason for the payment—these fields are optional.

output sequence (i.e., the exact order of the transmission within the day's total volume of transmissions). SWIFT officials have resisted attempts by law enforcement officials to gain access to the records because of the potentially large number of such requests. SWIFT points out that the sending or receiving bank will have better access to records about such messages.[24] This, and the problem of encryption, means that a bank-based monitoring or screening system, such as the systems outlined in chapter 7 of this report, would have to operate at each of the 450 banks using SWIFT rather than at a central SWIFT facility.

## NEW WIRE TRANSFER REGULATIONS

Law enforcement agencies would like to have easier access to wire transfer records and to have the information content of the records increased; they also would like to see monitoring systems that tag certain suspect accounts so that transfers to or from those accounts could automatically be called to their attention.[25]

In 1988, the Treasury Department's Office of Financial Enforcement began asking banks to report voluntarily any suspicious funds transfers or patterns of funds transfers. Given the volume of funds transfers and the highly automated process of transmittal, this was ineffective. In September 1993, the Department of the Treasury and the Federal Reserve Board jointly published proposed regulations to improve the usefulness of wire transfer records in control of money laundering, as had been mandated by the Annunzio-Wylie Act of 1992.[26]

Treasury had always required that wire transfers be kept as part of deposit account records, but had not mandated the form in which records were kept or how they could be retrieved. The proposed regulations did not mandate regular reporting to the government, but required that records contain standardized information and be maintained for five years in readily retrievable (but unspecified) form. For most banks, this would mean computer retrieval, but small banks with little traffic could still use other means of retrieval.

The new regulations were to have become effective on December 31, 1993, after a period for public comment. About 300 highly critical comments were received, and the regulations were held back for thorough revision.[27] They were issued in final form on January 3, 1995.[28] Treasury Under Secretary Ron Noble said, "These regulations mark a basic shift of our attention from cash

---

[24] Douglas Jeffrey, Regional Director, SWIFT Pan Americas, telephone discussion, Aug. 8, 1994.

[25] Based on interviews in the Money Laundering Section, Criminal Division, Department of Justice; Office of Financial Operations, Drug Enforcement Administration; the U.S. Customs Service, and several municipal and state law enforcement officials.

[26] *Federal Register* 46014, 46021, 46024.

[27] Most of the objections were based on the potential costs to banks of compliance and the potential loss of international competitiveness and encouragement of offshore netting. For large New York banks, the estimated cost of compliance with the proposed regulations was $14 million to $20 million per year; for a medium size bank $7 million, and for small community banks, $106,000. These costs were extrapolated from a small survey by the Bankers' Association for Foreign Trade. The Independent Bankers Association of America (IBAA) estimated that for community banks the required new record-keeping would require an additional 2.5 to 3 man-hours per day and would raise the annual cost of BSA compliance for small banks (already $5,455, according to IBAA) to $6,412. These figures were cited in a letter from IBAA president James R. Lauffer to Peter Djinis of the Dept. of the Treasury and William Wiles, Secretary of the FRB, on Oct. 4, 1993. They were taken from a study commissioned by the IBAA: Grant Thornton, "Regulatory Burden: the Cost to Community Banks, January 1993." Because these estimates of the costs of compliance were commissioned by an interested association and have not been validated by regulators they must be taken with a grain of salt. However, the Department of the Treasury and the Federal Reserve System, which had proposed the regulations, eventually agreed that they were too demanding. (Interview with Roger Weiner, Deputy Director, Office of Financial Enforcement, Dept. of the Treasury, March 16, 1994.)

[28] Federal Reserve System and Department of the Treasury, Amendment to the Bank Secrecy Act Regulations Relating to Recordkeeping for Funds Transfers and Transmittals of Funds by Financial Institutions, Final Rule, *Federal Register* 60 (1):220, Jan. 3, 1995.

at the teller's window to concentrating on crime hidden in the details of legitimate commerce."

The first of the new regulations requires only a minimum of new information.[29] The second requires each bank involved in a wire transfer to include all identifying information in the payment order as sent to the next bank, so that the information "travels" with the payment order from beginning to end.

Some banks will need new systems capabilities for searching their database. Large money center banks may decide to refuse wire transfer service to non-account-holders, rather than to create new mechanisms for searching their records for them.[30] It appears, however, that officers of most large banks regard the new regulations as "livable" and the government's response to their earlier complaints as commendable.[31] Community banks, generally much smaller, still regard the regulations as excessively burdensome, according to their industry association, The Independent Bankers Association of America.

The rules apply not only to banks but to all domestic financial institutions. They do not however apply to foreign affiliates of U.S. banks, a very large loophole. The Treasury Department "expects" that those U.S. banks will put anti-laundering measures into effect in their foreign branches and offices as well as is practical.[32]

---

[29] As the regulations were first proposed, banks would have been obliged to record complete information about the originator of the transfer and the ultimate beneficiary. An intermediary bank would have to obtain this information from the sender, even if this required manual intervention. Banks protested that it would be impossible to get such information for transfers from countries with strong bank secrecy laws.

[30] Interview with Robert M. MacAlister, Vice President and Senior Associate Counsel, Chase Manhattan, Feb. 21, 1994; similar comments were heard in interviews with Citibank officials.

[31] Interview with John Byrne, General Counsel, American Bankers Association, Feb. 16, 1994. (It was, however, also Mr. Byrne's opinion that the new regulations "will have no effect on money laundering—foreign banks can always wire dirty money into the United States.") The Office of the Comptroller of the Currency agrees that the compliance "will not be unduly burdensome in light of law enforcement goals," and representatives of several large banks confirmed this in discussions with OTA.

[32] This information comes from "Answers to Congressional Questions to the Department of the Treasury," *in Federal Government's Response to Money Laundering*," *Hearings* before the Committee on Banking, Finance and Urban Affairs, U.S. House of Representatives, 103d Ccongress, 1st Session, May 25-26, 1993, pp. 340 ff.

# Money Laundering and Law Enforcement 3

This chapter describes the legal and institutional structure for control of money laundering at the national level. Special attention is given to the Financial Crimes Enforcement Network (FinCEN), an agency within the Department of Treasury that provides intelligence and analysis for federal, state, and local law enforcement agencies in control of financial crimes. FinCEN is a possible site for expanded monitoring of wire transfers, under some of the technological alternatives discussed in chapter 7.

## LAWS AND REGULATIONS

Until 1970, many banks had no compunctions about accepting large cash deposits even when the circumstances indicated that the origin of the cash was probably illegal activity. The ***Currency and Foreign Transactions Reporting Act,*** commonly known as the Bank Secrecy Act of 1970 (BSA),[1] was intended to deter tax evasion and money laundering by creating an audit trail that would allow law enforcement agents to track large cash transactions.[2] Although it did not outlaw money laundering as such, it




[1] P.L. 91-508, Title II, ( 31 U.S.C., Secs. 5311-5326)

[2] Eight years later, the Right to Financial Privacy Act directly regulated governmental and private sector use of financial records. It provided that banks can release the records only under subpoena or with customer consent, and except for special circumstances, the customer must be notified of and have the opportunity to challenge a law enforcement request. The act also set conditions under which law enforcement and regulatory agencies can share financial records—generally, the agency must have a legitimate need for the information, and the subject must be informed of the sharing of information and the justification of it.

created an expectation that banks would be vigilant in identifying suspect customers and transactions.

Under the BSA, the Department of the Treasury promulgated reporting requirements for financial institutions. For every cash transaction over $10,000, banks must file a Currency Transaction Report (CTR); casinos similarly must report such transactions with the Internal Revenue Service (IRS) on a Currency Transaction Report by Casino (CTRC). Persons who export or import over $10,000 in cash or monetary instruments must file an International Transportation of Currency or Monetary Instruments Report (CMIR). U.S. citizens or residents must report foreign bank accounts by filing a Foreign Bank and Financial Accounts Report (FBAR). In 1984, an additional IRS requirement was imposed; businesses other than financial institutions (for example, automobile dealers) must report cash transactions of over $10,000 by filing an IRS form 8300.[3] Bank regulators monitor banks' compliance with BSA rules. IRS is responsible for monitoring compliance by nonbank financial institutions[4] (see table 3-1).

Although the BSA made a bank's failure to file a CTR a crime, money laundering itself was not a crime until the ***Money Laundering Control Act of 1986***.[5] This statute fully criminalized money laundering, with penalties of up to 20 years and fines of up to $500,000 for each count. It also did several other things:

- made helping money launderers a crime,
- outlawed structuring or "smurfing" operations (i.e., breaking large cash deposits into several deposits of less than $10,000 in order to avoid reporting requirements),
- extended criminality to persons knowingly engaging in financial transactions with money generated by certain crimes, and persons who are "willfully blind to" such unlawful activity,[6] and
- mandated compliance procedures to be required of banks; the procedures were spelled out in 1987 regulations.

The ***Anti-Drug Abuse Act of 1988*** increased the civil and criminal penalties for money laundering and other BSA violations, to include forfeiture of any property or assets involved in an illegal transaction related to money laundering. The act gave the Treasury Department the power to require financial institutions in geographically defined areas to file additional transaction reports for purposes of law enforcement. It also directed the

---

[3] A revised version of Form 8300 was issued in September 1994. The primary change, reflecting a change in statutory requirements, was the expansion of the definition of "cash" to include foreign currency and certain monetary instruments as well as U.S. currency, and to require filers to specify the kind of "cash" they received. Form 8300 is regarded as tax information and is therefore not available to law enforcement except for federal tax investigators.

[4] From 1988 through 1992, the number of Form 8300s filed steadily increased, as the IRS mounted well-publicized compliance checks. After these were discontinued for budgetary reasons, the number of Form 8300s filed fell by nearly 15 percent in 1993-1994, at a time when CTR filings strongly increased. In spite of a widely publicized prosecution of an automobile dealership that repeatedly accepted cash payments for expensive automobiles from suspected drug dealers without reporting the transactions, only 117,000 Form 8300 forms were filed in 1994, a 16 percent decrease from the 1993 volume.

[5] Title I, Subtitle H of the Anti-Drug Abuse Act of 1986, P.L. 99-570.

[6] Section 1957 (18 U.S.C. § 1957 (Supp. IV 1986), "Engaging in monetary transactions in property derived from specified unlawful activity," applies to people with knowledge or reason to know that the funds were derived from illegal activity, but does not require an intent to promote money laundering. It contained an exemption for bona fide attorneys' fees until 10 days before the President signed the Bill. The Senate had adopted the exemption because of concern about the right to effective assistance to counsel and the question did not arise during House debate. However, the exemption was dropped from the bill during a late night conference to resolve differences between Senate and House versions, not because conferees disagreed with the intent but because of the fear that other situations also might warrant special treatment. The issue of statutory exemptions was explicitly left for a later Congress. ("Making Criminal Defense a Crime Under 18 U.S.C. Section 1957"), 41 *Vanderbilt Law Review* (1988), 843-849. It is now interpreted as not applying to fees for a lawyer defending a person indicted for money laundering or drug trafficking.

TABLE 3–1: Bank Secrecy Act (BSA) Reporting Requirements

| Name of report | Who must report | Subject of report | Receiving agency | Form no. |
|---|---|---|---|---|
| Currency Transaction Report (CTR) | Financial institutions | Cash Transactions $10,000 or over | Internal Revenue Service | Form 4789 |
| International Transportation of Currency or Monetary instruments Report (CMIR) | Person transporting funds from or into country | Cash or monetary instrument of $10,000 or more being taken into or out of country | U.S. Customs Service | Form 4790 |
| Currency Transaction Report by Casinos (CTRC) | Licensed casinos with annual gaming revenue over $1 million | Currency transaction in excess of $10,000 | Internal Revenue Service. Those in Nevada file with State Gaming Control Board | Form 8362 |
| Foreign Bank and Financial Accounts Report (FBAR) | Persons subject to jurisdiction of the U.S. | All foreign bank, securities, or other financial account that exceeds $10,000 during calendar year | US Dept. of the Treasury | Form 90-22.1 |
| Report of Cash Payments Received in a Trade or Business | Any trade or business | Cash payment in excess or $10,000 | Internal Revenue Service | Form 8300 |

SOURCE. Office of Technology Assessment, 1995

Department of the Treasury to negotiate bilateral agreements covering the recording of currency transactions and the sharing of this information among governments.

The ***Depository Institution Money Laundering Amendment Act of 1990*** gave the federal government authority to request the assistance of a foreign banking authority in investigations and law enforcement, and to accommodate such requests from foreign authorities.

The ***Annunzio-Wylie Anti-Money Laundering Act of 1992***[7] requires financial institutions to have compliance procedures and staff training. Bank charters can be revoked, or their coverage by Federal Deposit Insurance can be terminated, if they are convicted of noncompliance.[8] These sanctions are so powerful that, according to bank regulators, they are unlikely to be sought often.

The huge volume of CTRs now far exceeds the resources that law enforcement agencies have for investigating them. The ***Money Laundering Suppression Act of 1994*** was designed to reduce the number of CTRs by about 30 percent annually, by mandating certain exemptions. This act also requires federal registration of all nonbanking money transmitters, or business enterprises that cash checks, transmit money, or exchange currency. This may include 10,000 American Express agents, 14,000 Western Union agents, 45,000 agents of Traveler's Express, and all *casas de cambio* (currency exchange houses) and *giro* houses (money transmitters). The Treasury Department can require the reporting of monetary instruments drawn on or by foreign financial institutions. States are asked to draft uniform laws

[7] Part of the Housing and Community Development Act.

[8] The banking industry generally accepted and even supported this legislation because regulators were given the flexibility to consider a broad range of factors and mitigating circumstances before closing a bank, according to a statement of the American Bankers Association (ABA) on Current Trends in Money Laundering, for the United States Senate, Committee on Government Affairs, Permanent Subcommittee on Investigations, Feb. 27, 1992 (ABA ins).

covering the licensing of nonbank money transmitters.

Since 1988, property or assets involved in specified illegal transactions can be forfeited and part of them can be used to pay for the prosecution. Law enforcement agencies enthusiastically grasped this new weapon,[9] and sharing of these seized assets was held out as an inducement to informers, and even to foreign governments to encourage them to cooperate in anti-laundering law enforcement efforts.[10] In 1994, total proceeds from cash and property seized amounted to nearly $550 million; from 1985 through 1994, the Department of Justice won forfeiture of more than $3.8 billion plus additional unsold property appraised at $277.7 million.[11]

Provisions related to asset seizure are framed very broadly.[12] In *United States* v. *Daccarett* a federal appellate court ruled that the warrantless seizure of wire transfers does not violate the Fourth Amendment ". . . when the Attorney General has probable cause to believe that property is subject to civil forfeiture."[13] Recently, however, there has been criticism of the aggressive use of asset seizure. In late 1992, three Supreme Court cases significantly tightened the conditions for forfeiture.[14] This action may indicate that the Supreme Court disapproves of the Justice Department's and other prosecutors' aggressive interpretation of forfeiture.

Perhaps most significantly, in *United States* v. *$405,089.23*, the Ninth Circuit ruled that a civil forfeiture following a criminal conviction for drug charges constituted a second punishment proscribed by the Double Jeopardy Clause of the Sixth Amendment and overturned the asset forfeiture.[15] This decision has spawned a slew of Double Jeopardy challenges in the Ninth Circuit.[16] The flip side of this ruling would imperil criminal prosecutions following civil forfeitures, greatly undercutting one of the benefits of a wire

---

[9] U.S. Congress, House of Representatives, Committee on Banking, Finance, and Urban Affairs, "Federal Government's Response to Money Laundering," *Hearings* 103rd Congress lst Sess., May-25-26, 1993. Testimony of Peter Djinnis, Director of Office of Financial Enforcement, Dept. of Treasury.

[10] For a detailed discussion, see S.M. Warner, "Due Process in Federal Asset Forfeiture," *Criminal Justice*, v.8, No.4, Winter 1994, pp. 14-19, ff.

[11] Information provided by the Executive Office of Asset Forfeiture, Department of Justice, Jan. 13, 1995. The provision allowing seized funds to offset the cost of prosecution expired in December 1993 but was later reinstated.

[12] Some have even advocated that the tool be used to reduce environmental degradation, on the grounds that since it is a criminal offense to knowingly engage in a financial transaction involving the proceeds of specified unlawful activity, a bank may be held liable if it funds corporate activities of any corporation it knows to be in violation of the Clean Air Act. (Gordon Greenberg and Wobert W. Blanchard, "When Money Laundering Law Meets Environmental Risks," *ABA Banking Journal*, July 1992).

[13] Gregory Wilson, "The Changing Game: the United States Evolving Supply-Side Approach to Narcotics Trafficking," *Vanderbilt Journal of Transnational Law*, v. 26, January 1994, 1163-1209.

[14] In *United States* v. *92 Buena Vista Avenue*, the government argued that an "innocent owner" defense should not be allowed because the title to the proceeds of crime is vested in government immediately on the commission of the crime (the "relation-back doctrine"). The Court affirmed the "relation-back" doctrine but said the innocent-owner defense holds until the government is granted a judgment of forfeiture. In *Alexande* v. *United States* (criminal forfeiture) and *Austin* v. *United States* (civil forfeiture) the Court ruled that forfeitures may constitute punishment and may be subject to limitation under the Excessive Fines clause of the Eighth Amendment. The Court held in *United States* v. *James Daniel Good Real Property* that a right to notice and opportunity for a hearing in real estate forfeiture rests solidly on the due process clause of the Fifth Amendment. The Court has still to hear arguments on whether convicted drug dealers are entitled to advance notice and a hearing before seizure of their property, as the Ninth Court of Appeals has ruled (*United States* v. *Good)*. Richard C. Reuben, "Putting the Brakes on Forfeiture," *American Bar Association Journal* 80, February 1994, p.116.

[15] 33 F.3d 1210 (9th Cir. 1994).

[16] Including federal cases outside the Ninth Circuit, in the first six months of 1995, at least 40 cases have been decided alleging Double Jeopardy violations.

transfer monitoring system, namely, more efficient and effective asset forfeiture.

## FEDERAL AGENCIES' ROLES AND RESPONSIBILITIES

Several federal law enforcement agencies are involved in control of money laundering. They include, within the Department of Justice, the Federal Bureau of Investigations (FBI) and the Drug Enforcement Administration (DEA); and, within the Department of the Treasury, the Internal Revenue Service (IRS) and the U.S. Customs Service.

Each of these law enforcement agencies has an intelligence capability, but the agencies are further backed up by a shared information-development unit—namely, the Financial Crimes Enforcement Network (FinCEN) an analytical unit within the Department of the Treasury. There is also communication between law enforcement and national security agencies. FinCEN has been proposed as the locus for responsibility for monitoring wire transfers with the technical systems assessed in this report. For that reason, FinCEN is described in detail in this chapter.

The compliance of financial institutions with money laundering statutes is monitored by five federal regulatory agencies:

- the Office of the Comptroller of the Currency,
- the Board of Governors of the Federal Reserve System,[17]
- the Office of Thrift Supervision,
- the National Credit Union Administration, and
- the Federal Deposit Insurance Corporation.

Most large-scale money laundering control initiatives are intended to be multiagency efforts. In practice, investigations are usually initiated by one agency on the basis of information provided by informants and field agents, BSA reports, or referrals from financial institutions or bank examiners. There has often been a great deal of "turf defending" on the part of the agencies. In part, this was inevitable because money laundering is related to a great many "specified unlawful activities" or predicate crimes, many of which are the specific responsibility of a particular law enforcement agency. In part, the tension is also a byproduct of the high value each law enforcement agency places on protecting its undercover agents and operations and the identity of established informers; information must be closely held to reduce inadvertent leaks.

In 1987, an agreement was entered into by the Departments of Treasury and Justice about their overlapping responsibilities, supplemented by a 1990 Memorandum of Understanding among those Departments and the U.S. Postal Service. Other mechanisms for cooperation have been developed for attempting to coordinate anti-money-laundering efforts:

- The Office of National Drug Control Policy (ONDCP) in the Executive Office of the President attempts to develop overall policy directions for drug control and control of drug-related money laundering.
- The Multiagency Financial Investigations Center (MAFIC) is a coordinating mechanism for the DEA, IRS, FBI, U.S. Customs Service, and the Postal Authority.
- There are several "High-Intensity Drug Trafficking Area" (HIDTA) task forces made up of IRS and DEA agents.
- The Organized Crime Drug Enforcement Task Force program, composed of federal, state, and local agencies organized into 13 regional task forces, has conducted a number of successful and highly publicized operations known by

[17] The Federal Reserve regulates state-chartered banks, bank-holding companies, foreign banks operating in the United States, and Edge Act corporations set up by U.S. banks to conduct foreign business, about 1,300 institutions. The Office of the Comptroller of the Currency regulates federally chartered banks.

colorful names—Polar Cap, Greenback, Dinero, and Green Ice.[18]

- A very successful New York City law enforcement unit—the El Dorado task force—is made up of Customs Service and IRS agents together with state and local police.[19]
- Cooperation among the regulatory agencies is encouraged by the Bank Fraud Working Group and the Bank Secrecy Act Advisory Group (a nongovernmental panel of experts appointed by the Secretary of the Treasury).

The ONDCP strongly encouraged increased emphasis on the comprehensive collection, analysis, and sharing of information, especially that which sheds light on the structure of drug trafficking operations and organizations. This is often resisted by the agencies, in part because of differences in their organizational cultures (see table 3-2). Nevertheless, the law enforcement agencies insist that the historical problem of turf protection "is being effectively addressed today."[20]

The FBI has broad jurisdiction to investigate money laundering through a wide range of statutory violations involving specified underlying criminal activity.[21] This agency tends to focus on the underlying criminal activities, attempting to dismantle entire criminal organizations and jail their top leaders. Of the agency's six "priority areas that most affect society"—drugs, organized crime, white collar crime, terrorism, foreign intelligence, and violent crimes—at least the first four nearly always involve some money laundering, and the FBI is increasingly alert to the financial aspects of criminal organization. The FBI Laboratories' Racketeering Records Analysis Unit provides support to field divisions with its ability to trace the flow of illicit money through bank deposits, money orders, adding machine tapes, invoices, receipts, checks, bills of lading, and other financial records.[22]

The FBI signed a Memorandum of Understanding with representatives of the United Kingdom in late 1993 establishing a White Collar Crime Investigative Team, to cooperate on investigations and prosecutions in matters affecting the two countries and the Caribbean British Dependent Territories, including the Cayman Islands. The four-person team is based in Miami.

DEA, also in the Department of Justice, is the lead federal agency in enforcing narcotics and controlled substances laws and regulations. Through its Financial Investigations Section, DEA seeks to detect drug-related money laundering and encourage seizing the assets of drug traffickers. But its principal focus is on arresting drug dealers, and DEA tends to judge its operations by number of arrests.[23] In general, the two Depart-

---

[18] Tthe first phase of Green Ice, in 1992, targeted *casas de cambios* in the southwestern United States, and resulted in the arrest of 192 people in the United States, Canada, the United Kingdom, Italy, and Spain. In a second phase of Green Ice, undercover DEA agents created front corporations and offered them to drug traffickers to be used in money laundering. Money was transported physically to Mexican banks and subsequently wired into accounts held by the DEA agents. In other operations, money was picked up from locations in the United States and Canada, deposited in banks, and wire transferred to Colombia. The second phase of Green Ice ended in early April 1995, and resulted in the arrest and charging of 80 people. In the course of Green Ice, the government seized $60.3 million, plus 14,000 pounds of cocaine and 17 pounds of heroin. (Press Release from the Office of the U.S. Attorney for the Southern District of California, Apr. 3, 1995.)

[19] The participation of state and local officers is said to be especially valuable because they can arrest for some non-federal crimes such as illegal possession of weapons.

[20] Jeff Ross, Acting Chief of the Money Laundering Section of the Department of Justice (letter to OTA, Apr. 14, 1995) .

[21] The Department of Justice has a Money Laundering Section within its Criminal Division; a proposal by the Attorney General (Dec. 9, 1994) to integrate this group into the Civil Assets Forfeiture Section, is pending before Congress.

[22] OTA interviews with RRAU/FBI August 18, 1994; see also J.O. II Beasley, "Analysis of Illicit Drug and Money Laundering Records," *Narc Officer*, Oct. 1990, p. 31.

[23] David Kennedy, *On the Kindness of Strangers: The Origins and Early Days of FinCEN*. Case Program, John F. Kennedy School of Government, Harvard University, 1991. Kennedy characterizes DEA as "street-smart door-kickers."

TABLE 3-2: Federal Law Enforcement Agencies: Organizational Culture and Approaches to Money Laundering

| Federal agency | Primary goals | Assumptions about money laundering |
|---|---|---|
| Federal Bureau of Investigations (Dept. of Justice) | "Emphasis on wholesale and complete dismantling of criminal organizations."a Tries to attack the organization itself, through its leadership. Requires much information about structure and behavior of organization's leaders. Typical mode: long operations with sudden, well-prepared wrapup. | Money laundering IS a symptom of the underlying disease,"[a] Attention to money laundering IS primarily in order to track or understand structure of the criminal organization and locate its leadership. |
| Drug Enforcement Administration (Dept. of Justice) | Specialized to enforce laws against drug trafficking. Emphasis on arrests of malefactor and seizure of drugs and assets. Typical mode: frequent street "busts." Emphasis primarily on good field work, including undercover operations; secondarily on centralized strategic intelligence | Growing acceptance that emphasis on money laundering is an effective way to disrupt and harass drug operations. |
| Internal Revenue Service, Criminal Investigations Division (Dept. of the Treasury) | Objective is to stop tax evasion. Uses undercover operations, etc., but primary mode is financial intelligence. | Targets financial crimes (money laundering, fraud, etc.) because they result in loss of tax revenue, but also investigates Specified Unlawful Activities often linked to money laundering |
| U.S. Customs Service (Dept. of the Treasury) | Charged with enforcing customs and other laws relating to collecting revenue from imports (duties). Also charged with interdicting and seizing contraband, including illegal drugs. In addition to border inspections, uses undercover operations and "busts," emphasizes arrests and seizures of money and drugs. | Primary target is smuggling of currency and monetary instruments, but also stresses use of financial Intelligence (including wire transfer data if available) as a means of Identifying and locating criminals. Oriented toward financial crime like other Treasury agencies; oriented toward field work and undercover operations like Justice agencies |
| Financial Crimes Enforcement Network (FinCEN) (Dept. of the Treasury) | Provision of strategic and tactical intelligence about financial transactions and relationships to law enforcement agencies (federal, state, and local); based on analysis of BSA data and mining of wide range of government and commercial databases | Detection and analysis of money laundering can provide the key to control of crimes for profit. Sharing of information benefits all law enforcement efforts. |

[a] David Kennedy, On the Kindness of Strangers: The Origins and Early Days of FinCEN Case Program, John F Kenedy School of Government, Harvard University, 1992. This table relies heavily but not exclusively on Kennedy's analysis.

SOURCE: Office of Technology Assessment, 1995

ment of Justice agencies see financial crime analysis as important but subordinate to the larger battle against drugs and organized crime.

Recognizing that crimes such as tax evasion and money laundering threaten the national financial system and its institutions, the Department of Treasury has an Under Secretary for Enforcement, elevated from the level of Assistant Secretary in 1994. Three operating bureaus—the U.S. Customs Service, the Secret Service, and the Bureau of Alcohol, Tobacco, and Firearms-have among their responsibilities some aspects of control of money laundering. The U.S. Customs Service has the primary responsibility for stopping the illegal crossborder flow of funds, both as smuggled currency (the Office of Inspections and Control) and as wire transfers and funds transmittals (the Office of Enforcement). The Secret Service and Bureau

of Alcohol, Tobacco, and Firearms concentrate more on counterfeiting but are sometimes called on to assist in anti-money-laundering operations.

Elsewhere in the Department of Treasury, the IRS has multiple responsibilities under the BSA. Its Criminal Investigations Division can initiate investigations of persons or organizations, including banks and brokerage houses, for possible criminal violations of the BSA.[24] The Criminal Investigations Division now has about 4,000 employees, nearly a quarter as many as are in IRS's Tax Collections Division.

The role of the IRS in pursuit of money launderers has greatly increased in recent years, largely at the behest of Congress.[25] That role is however controversial. The justification for IRS enforcement is that most kinds of money laundering result in tax evasion, and some money laundering is done for the specific purpose of tax evasion. A few extreme critics raise the question of whether it is right that some tax evaders—namely, those suspected of other crimes that have not been (and perhaps cannot be) proven—should be selected and given high priority for especially severe investigation and prosecution.[26] They argue that this is "targeting a special class of tax evaders for a special kind of tax enforcement by arbitrary administrative fiat,"[27] and they suggest that such sanctions could be, and perhaps have been, used against "political dissidents" such as civil rights protesters or antiwar activists.

## STATE LAW ENFORCEMENT

Twenty-three states have laws against money laundering; these differ somewhat as to the elements of the offense and as to penalties.[28] Not all of the states with money laundering laws have active enforcement programs. The most long-standing and well-developed programs are in Arizona, Texas, and California.[29]

Only a few states require currency transaction reporting by state-chartered banks. Under FinCEN's Project Gateway, states are able to receive electronically all CTRs pertinent to their jurisdiction.[30] Some states have laws that allow for confiscation of property obtained with funds from illegal activities. The Arizona Racketeering Act is one of the most comprehensive and effective.[31] Arizona has an aggressive multiagency anti-

---

[24] The exception is the smuggling of currency across borders, which is the responsibility of the Customs Service. Otherwise, the IRS shares responsibility for investigations with other law enforcement agencies. A Criminal Investigations Division strategy statement provided to OTA says that the IRS has the mission of "utilizing its statutory jurisdiction in concert with the financial investigative expertise of its special agents in conjunction with the efforts of other federal law enforcement agencies."

[25] According to some IRS officials, in discussion with OTA staff.

[26] This was the case, for example, when Al Capone was jailed for tax evasion.

[27] David Burnham, *A Law Unto Itself: the IRS and the Abuse of Power* (New York: Vintage Books, 1991), p. 76. Burnham likens this to past efforts to use IRS audits and prosecutions for general law enforcement purposes or, according to Burnham, for political purposes—against gambling, in the early 1950s under pressure from Senator Estes Kefaufer; against organized crime in the 1960s under Attorney General Robert Kennedy; against drug traffickers in the 1970s under President Nixon; and against war protestors and civil rights activists, also under President Nixon (pp. 90-98). Robert E. Powis, Dep. Asst. Secretary of the Treasury for Enforcement from 1981-1984, notes (approvingly) that under President Nixon "tax cases were successfully prosecuted where not enough evidence could be collected to make a drug case." Robert E. Powis, *The Money Launderers* (Chicago: Probus Publishing Co., 1992).

[28] General Accounting Office, *Money Laundering: State Efforts To Fight it Are Increasing but More Federal Help is Needed*, GAO/GGD-93-1, October 1992.

[29] These programs were developed under demonstration projects funded by the federal Bureau of Legal Assistance, Dept. of Justice. (Information provided by the Criminal Justice Project of the National Association of Attorneys General; Michael P. Hodge, Project Director, and Thomas R. Judd, Special Counsel, discussion on Aug. 9, 1994).

[30] At least seven states could do so at the end of 1994; the others are in the process of being brought online.

[31] Clifford Karchmer and Douglas Ruch, "State and Local Money Laundering Control Strategies," *National Institutes of Justice Research in Brief*, October 1992.

money-laundering program that includes experiments with the screening of international wire transfers.

## THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN)

FinCEN was set up within the Department of the Treasury by Executive Order in April 1990. The mission of FinCEN, described as a "multiagency support unit," is to support and assist federal, state, and local law enforcement agencies and regulators by providing information and analysis, and to identify targets for investigations of money laundering and other financial crimes. FinCEN's establishment reflected the conviction that the most effective way of disrupting organized crime is to cut off or seize the profits from illegal activities. FinCEN is "an intelligence operation dedicated to the analysis of the financing of criminal enterprises whatever their primary criminal activity (drugs, racketeering, vice, etc.)," and ". . . having the capacity and opportunity to ask deep structural questions about trends and practices in modern money laundering techniques."[32] FinCEN's organization and activities testify to the dominant role that computerized information and computer-supported analysis are coming to play in law enforcement—an importance that is sometimes resisted or denigrated by old line "street" law enforcement agents.

In late 1994, FinCEN absorbed the Treasury Department's Office of Financial Enforcement and was given the expanded mission of overseeing the full range of the Department's regulatory and enforcement responsibilities under the BSA (Bank Secrecy Act). FinCEN has a staff of 200, including 87 intelligence analysts and 23 agents—of these, 12 analysts and 22 agents are on temporary detail from law enforcement agencies.[33] It had been expected to grow steadily over its first four or five years as its advanced computer systems were developed or acquired and as federal and state agencies became accustomed to calling on its expertise. Budget restrictions and the movement to downsize the federal government have moderated FinCEN's anticipated growth somewhat but the budget was $21.2 million in FY 1994.

FinCEN analysts and agents support law enforcement in several ways:

- by using database searches to answer the requests of law enforcement agencies for information,
- by identifying suspected offenders by analyzing and relating multiple databases,
- by providing evidentiary and analytical support for ongoing investigations, and
- by developing and disseminating research and policy studies on money laundering enforcement.

The targeting of suspects is the most proactive of FinCEN's activities. In the first year that the proactive targeting system was in use, about 200 referrals were made; it is not known how many active investigations are underway as a result.[34]

In all of its work, FinCEN operates by integrating and analyzing information from a wide range of government and commercial sources, using advanced computer techniques—including many usually categorized as "artificial intelligence" (AI)—to link or relate disparate bits of data and thereby reveal relationships or patterns that are, or may be, indicative of illegal financial activities (see chapter 4 for details).

---

[32] Malcolm K. Sparrow, "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects," *Social Networks* 13 (1991), p. 261.

[33] As of January 1995.

[34] In response to one inquiry from federal agents in "a large Western city," FinCEN analysts identified 25 potential targets. After initial investigations in the field, FinCEN was asked to do further searches on seven of these, and eventually two multiagency investigations began. One of these has already resulted in identifying a narcotics ring for which money was being laundered, leading to arrests and seizure of cocaine.

The basic source of data is Treasury's financial database made up of those reports required by the BSA, and described earlier in this chapter.[35] FinCEN now receives and monitors all CTRs submitted by financial institutions, about 10 million a year.[36] In proactive targeting of suspects, FinCEN analysts use a system based on principles derived from artificial intelligence. The system links together transactions according to common subjects and accounts. Combining a variety of clues or "rules" worked out by the developers, it then performs an evaluation of suspiciousness for all subjects, accounts, and transactions. Analysts select the most suspicious subjects and accounts for further analysis, including matching them with information in a score of other government and commercial databases as shown in box 3-1, using link analysis. In this way an otherwise unknown subject, making a sizable cash deposit, may be linked through his/her account number, address, social security number, or company name to other transactions or other bank accounts, perhaps held by persons who are already known to law enforcers as suspects.

The computer program that supports this linking activity is known as the FinCEN Artificial Intelligence System (FAIS); it is a rule-based expert system. An early version was developed in the mid-1980s by investigators at the U.S. Customs Service. The Customs development group was transferred to FinCEN when it was created in 1990, and the system came into use in March, 1993 (see box 4-1 in chapter 4 for details). Development continues; the 400 "rules" on which the targeting system works are steadily being revised and improved.

Wire transfer records are not now accessible to FinCEN. The number of transfers made daily—now more than 700,000—is so large that the capacity of FinCEN's current systems would undoubtedly be far overwhelmed. However, if it were possible to reduce the amount of data to be manipulated by three-quarters—for example, by automatically exempting the records of transfers of well-known corporations and financial institutions—it might be possible to match the remaining 25 percent against CTR records and where there is an apparent match, call out additional information from FinCEN's other database sources.

FinCEN systems developers base their systems on a modular client-server architecture with personal computers as the primary analyst work station, and a local area network for connectivity. They emphasize the maximum use of off-the-shelf commercial or government-developed software. Telecommunications channels into FinCEN and the ability of outsiders to dial up FinCEN computers and databases is tightly controlled in the interests of information privacy, security and integrity.

Other computer projects developed by FinCEN to support law enforcement include Project Gateway and the Criminal Referral System. The first allows State law enforcement coordinators (the designated contacts between State agencies and FinCEN) to access directly the IRS Financial Database of CTRs and other BSA reports. All but four states are now online, and access is currently being developed for those four. The Criminal Referral System will contain Criminal Referral and Suspicious Transaction Reports (described in chapter 1) identifying bank employees, bank customers, or others that have been the subject of

[35] FinCEN's authority to receive and use Form 8300 data—data from the forms filed by nonfinancial institutions, such as car dealers, to report large cash transaction—expired in November 1992. These data are considered to be tax information, and access is therefore legally limited. Legislation to renew FinCEN's access has been proposed but is still pending. Currency and Monetary Instrument Reports (CMIRs), Customs Service forms for reporting funds being carried out of the country, are available to FinCEN electronically through the Customs Service's Financial Databases.

[36] About two years of CTR data are stored on the system; eventually there will be five years of data.

## BOX 3-1: Databases Used by FinCEN

**Government Databases:**

- Department of the Treasury Financial Database: Currency Transaction Reports (CTRs), Casino Currency Transaction Reports (CTRCs), and other reports required under the Bank Secrecy Act (BSA)
- Treasury Enforcement Communications System: individual travel records, private aircraft entry records, importers and exporters
- Postal Inspection Service: records of open and closed criminal cases involving postal fraud and related crimes
- Interpol Case Tracking System: international criminal case records
- Narcotics and Dangerous Drugs Information System: case files of the Drug Enforcement Administration
- U.S. Customs Service Automated Commercial Data System: data on exports and imports
- Immigration Service: student visas held by nonimmigrants
- Department of the Treasury: lists of purchasers of U.S. Treasury bills and bonds
- U.S. Department of Agriculture: records of foreign nationals purchasing U.S. property
- Metromail: all U.S. mail directories, forwarding information, changes of address requests to major publishers, records of who lives at what address, and for how long
- Courthouse records: real estate information for many counties and cities in 11 states, listing owners (name and address), sales, etc.
- Bureau of Public Debt records

**Commercial Databases:**

- Dunn & Bradstreet: U.S. corporate registrations, officers, etc.
- Dunn & Bradstreet International: same as above
- LEXIS/NEXIS: legal briefs, court decisions, public filings, newspaper and magazine articles
- National Association of Securities Dealers (NASDA):[1] licensed brokers/dealers of over-the-counter stocks, disciplinary actions against them
- CBI-IDENT/DTEC: a credit bureau from which FinCEN can get identifying information on individuals, including name, address (current and past), and social security number, but cannot access credit history
- InfoSouth: stores and searches news articles from many South American countries
- Information America: corporate records, including location, officers and partners, registered agents, liens and judgments, SEC filings, bankruptcy records, etc.
- Invest/Net: Information about companies required to file with the Securities and Exchange Commission, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision
- National Center for Missing and Exploited Children: cases.
- Phonedisk: addresses and phone numbers in New York and New England
- Printice Hall On Line: corporate information, bankruptcies, tax liens, judgments, foreclosures, plaintiff and defendant listings
- TRW-Sherlock: a credit bureau from which FinCEN can get identifying information on individuals, including name, address (current and past), and social security number, but cannot access credit history.

[1] The National Association of Securities Dealers is a self-governing organization of dealers of over-the-counter (i.e., non-exchange-listed) stocks

SOURCE: Financial Crimes Enforcement Network (FinCEN), *Annual Report,* September 1993.

BSA reports, investigations, or prosecutions. When the Criminal Referral System becomes fully operational,[37] it will first allow online access to five regulatory agencies overseeing financial institutions.[38] A second phase of the development will provide on-line access for federal law enforcement agencies.

Further down the road are other analytical support systems, including:

- An autoquery prototype that will allow users to type in a name, account number, or other identifiers and automatically locate and abstract related information from all databases (the system is intended to cut analysts' time for performing these tasks by two-thirds); and
- a text-retrieval system to scan in and search documents such as indictments.

In addition to direct services in response to law enforcement inquiries, FinCEN services and products include:

- analyses of Federal Reserve Bank data on the shipment of currency from and to member financial institutions (analyses are performed by geographical region to identify "abnormalities" such as an unexplained surplus of cash in one location);
- "threat assessments," or evaluations of likelihood of money laundering activity, for states that are considering anti-money-laundering programs, or are seeking to improve the allocation of law enforcement resources; and
- assessments of money laundering by country.

In FY 1994, its third full year of operation, FinCEN received 6,153 inquiries from 158 law enforcement agencies.[39] In spite of some clear successes, evaluation of FinCEN's help to law enforcers is difficult. FinCEN itself has little direct feedback from clients and thus little knowledge of the results of its referrals. Some field level law enforcement agents are skeptical; some told OTA that they have not been aware of any assistance from the agency. IRS, Customs, DEA, and FBI agents who have worked "on the street" or mounted active operations told OTA that they relied much more heavily on their own agencies' intelligence units, on undercover agents, or on tips from informants. However, there may be reasons for this; leads generated by FinCEN may be passed through higher levels of a user agency to its agents without being identified as to source. FinCEN information may be discounted or ignored by some agents who are not used to dealing with that kind of data. Some agents who talked with OTA had not been on the street for several years, and FinCEN's most sophisticated products have been introduced in the last year or two. Higher level comments may well be intended to protect an agency's own image and budget.

Outside of law enforcement, some FinCEN critics have charged that the agency's activities constitute systematic violation of citizens' privacy.[40] More moderate privacy experts still view the manipulation and matching of information from many databases to reveal a complex pattern of financial activity by an individual, as a substantial

---

[37] The Criminal Referral System was to have become operational in early 1994 but was delayed by a series of decisions increasing the number of agencies to be served, the data to be included, and the reporting thresholds. It is now expected to be operational in September 1995.

[38] These are the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Office of Thrift Supervision, the Federal Deposit Insurance Corporation, and the National Credit Union Administration.

[39] About 20 percent of these inquiries were from local and state agencies, 77 percent from federal agencies, and 3 percent (214 inquiries) from international agencies.

[40] For example, Jeffrey Rothfeder, a journalist and privacy advocate, charges that FinCEN . . ."creates files on financially active individuals; these files are then electronically overlaid with information on individuals taken from supposedly secure federal databanks, which FinCEN has immediate online access to . . ." and, Rothfeder concludes, FinCEN may therefore have invaded the privacy of "millions of innocent Americans" by putting them under surveillance. Jeffrey Rothfeder, *Privacy for Sale (*New York: Simon & Schuster, 1992).

intrusion on citizens privacy[41] (see chapter 5 for discussion of financial privacy). Especially as FinCEN opens up its databases to state and local law enforcement officials, the possibility of gross violations of financial privacy may increase.[42] On the other hand, there have been a number of legislative and administrative attempts to expand FinCEN's power by fully exempting it from the provisions of both the Privacy Act and the Right to Financial Privacy Act.[43]

Because of the international dimension of much financial crime, FinCEN needs to cooperate with law enforcement agencies in other countries. Such cooperation is often complicated by the fact that some countries have privacy laws more stringent than those in the United States, that prohibit or limit the sharing of financial data, even for law enforcement purposes. (These issues are discussed in chapters 5 and 6.) FinCEN can share BSA data with other countries on the authority of the FinCEN director; however, to share the information in the other government databases that it uses, FinCEN must get permission from the agencies that own the data.

FinCEN has close liaison with the international Financial Action Task Force (FATF), and Interpol (see chapter 6). It has cooperative agreements with agencies similar to itself in several countries—AUSTRAC in Australia (described below) and TracFin in France.

AUSTRAC (the Australian Transaction Reports and Analysis Centre) is Australia's federal agency for recording and analyzing financial records, closely analogous to FinCEN. AUSTRAC collects and analyzes three types of data: 1) large cash transactions (including domestic and cross-border transactions and federal bank system cash reserves), 2) international wire transfers, and 3) reports of suspicious transactions. Large cash transactions are reported to the agency under the Financial Transaction Reports Act (FTR), which is similar to the U.S. Bank Secrecy Act. The FTR was amended in 1992 to require records of international wire transfers also to be forwarded to AUSTRAC.[44] (Domestic and bank-to-bank transfers not on behalf of customers are excluded.) The agency also integrates data that indicates the amounts of cash that financial institutions are transferring from and back to the Bank of Australia (Australia's central bank). This helps to identify institutions where large cash transactions are not being accurately reported. AUSTRAC thus uses much the same techniques that FinCEN relies on—i.e., relating disparate bits of financial information from multiple databases—but has the additional capability of adding wire transfer information.

The AUSTRAC system for analyzing wire transfer appears to be a close analog to the proposed U.S. wire transfer analysis system, although operational problems imposed by scale differences in the two countries' banking systems and economies are significant (see chapter 4). AUSTRAC receives reports of all international wire transfers, known as International Funds Transfer Instructions, within 24 hours of their transmission. An Electronic Data Delivery System (EDDS) allows automated transfer of this data to AUSTRAC from financial institutions, which run EDDS software on IBM-compatible computers equipped with a modem. Data is down-

---

[41] L. Richard Fischer, *The Law of Financial Privacy: A Compliance Guide* (2nd ed.) (Boston: MA: Warren, Gorham, & Lamont, 1991) 2:03 (1), 2-11.

[42] Professor Joel Reidenberg of Fordham University School of Law cautioned OTA workshop participants (Sept. 28, 1994) that the expansion of FinCEN's work in the area of data matching and transaction profiling may violate the spirit of the Right to Financial Privacy Act, to the extent that law enforcement "seeks to re-create an individual's transaction patterns" without the authority of a court order.

[43] Matthew N. Kleiman, "The Right to Financial Privacy vs. Computerized Law Enforcement, a New Fight in an Old Battle," *Northwestern University Law Review* 86, no. 4, Summer 1992.

[44] AUSTRAC was originally known as the Cash Transaction Reports Agency; the name was changed when analysis of wire transfers was added to its mission in late 1992.

loaded to AUSTRAC daily. The system imposes minimal requirements on financial institutions, according to AUSTRAC.

AUSTRAC integrates all of the financial data into a single database, and can retrieve it through a single query through the Transaction Reports Analysis and Query (TRAQ) system. TRAQ consists of three subsystems: basic query, report preparation, and automated screening. The latter subsystem, called ScreenIT, automatically screens FTR information for unusual transactions that may be of interest to Australian taxation or law enforcement agencies.

ScreenIT is a knowledge-based application that couples state-of-the-art computing with the pooled knowledge and experience of Australia's law enforcement and tax agencies, by whom it was developed.[45] It extracts from the financial databases specific pieces of information that meet criteria set by these agencies. The objective in developing the system was to have it "automatically detect information on major unusual transactions. . . ." The items that are flagged often have to do with shell corporations, tax shelter and bank secrecy countries, structuring of deposits and irregularities in relation to international trade, especially when related to persons already under investigation or previously identified as suspicious.

AUSTRAC officials believe that the ScreenIT system has proven valuable. There have been a number of informal indicators that the system is successful at identifying suspicious transactions. In some cases, suspicious activities by particular individuals have been identified by both ScreenIT and by suspicious transaction reports issued by financial institutions. ScreenIT has also identified cases involving persons already under investigation by domestic and/or international law enforcement organizations. Finally, feedback from AUSTRAC's clients has been positive.

The Australian Taxation Office (similar to the U.S. IRS) and Australian law enforcement agencies have had online access to FTR information since 1990, and access to International Funds Transfer Instructions (IFTI) and other FTR information since the second half of 1993.

It must be emphasized, however, that the problem of monitoring of wire transfers in Australia and the United States is very different in scale. In Australia, there are approximately 20,000 wire transfers daily, as compared with perhaps 700,000 in the United States. In Australia, moreover, approximately 90 percent of all reportable international wire transfers pass through only four large banks rather than the 10 to 20 money center banks that participate in the United States.

## SUMMARY

Law enforcement agencies traditionally attempted to track money laundering in order to detect and document an underlying crime. The attractiveness of this strategy grew as frustration developed over failed attempts to stop drug trafficking, and further increased as the role of money laundering in terrorism, illegal arms trading, and white collar crime was realized. A series of laws gradually criminalized activities related to money laundering, and expanded civil procedures—notably asset forfeiture—provided other weapons for controlling money laundering. However, some of these tactics—including tax evasion prosecution and asset forfeiture—together with proposals for increased monitoring of financial records, have aroused criticism. This is an area where there is strong tension between the need for effective law enforcement and the desire to limit police

[45] Graham Pinner, Deputy Director, AUSTRAC, personal communication, Aug. 1, 1994. The development of ScreenIT was supported by several agencies, beginning in late 1992. These agencies were: the Australian Securities Commission, Australian Federal Police, National Crime Authority, Australian Customs Service, Australian Taxation Office, and AUSTRAC. The agencies formed a management group to guide development of the system and to evaluate the information produced by the system. In October 1993, the management group began evaluating information produced by a prototype system. Five months later, the ScreenIT Management Group unanimously agreed that the system was successful in identifying potentially nefarious activity and that use of the system should move into an operational phase."

power in the interest of individual privacy and autonomy. The use of computerized surveillance of financial transactions could exacerbate these tensions.

The institutional responsibility for federal anti-money-laundering efforts is dispersed, but there are a number of mechanisms for interagency cooperation. State and local anti-money-laundering programs are for the most part at an early stage of development. Because of the national and international dimensions of money laundering, federal leadership in its control is critical, as is coordination among federal civilian law enforcement agencies, intelligence agencies, local police, and federal and state bank regulators.

One institution that could play a central role in computer-assisted monitoring of wire transfer records is FinCEN, and a model for this involvement exists—Australia's AUSTRAC. However, giving this expanded responsibility to FinCEN could require an order of magnitude increase in the agency's resources. Many law enforcement officers, especially those in the field, question whether the results would justify the allocation of resources; but this may reflect a parochial point of view. Other critics of FinCEN object because of the implied invasion of individual privacy and corporate confidentiality.

# Technologies for Detecting Money Laundering

# 4

At the core of all wire transfer monitoring proposals are one or more computer technologies. Many of these technologies rely upon techniques developed in the field of artificial intelligence (AI). Others involve computer graphics and statistical computing. Wire transfer monitoring proposals generally involve a combination of technologies, institutional structures, and reporting requirements. Four of these combinations are presented as options in chapter 7. However, a limited set of technologies and their relative capabilities form the core of each option.

This chapter discusses two topics central to understanding these technical options and the policies surrounding their use. The first section introduces several basic technologies that are employed in one or more options. The second section discusses challenges that must be overcome by all options. These challenges involve characteristics of wire transfer data and money laundering profiles.

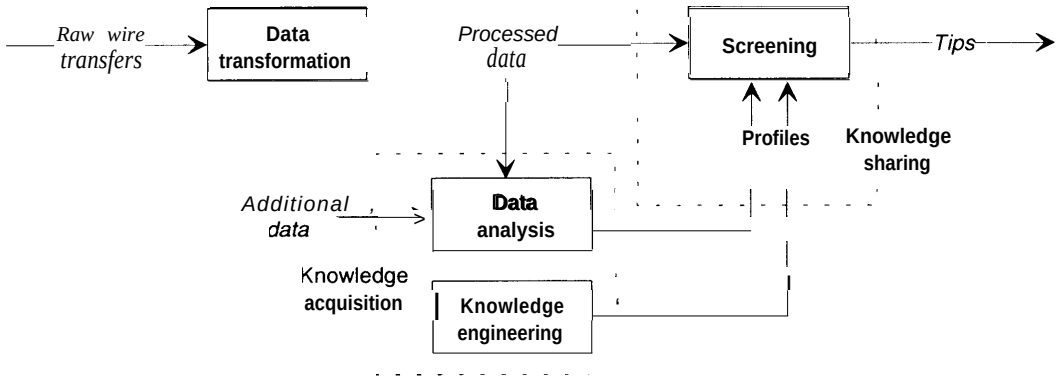


## BASIC TECHNOLOGIES

There are at least four categories of technologies that may be useful in the analysis of wire transfers. These technologies can be classified by the task they are designed to accomplish:

- *wire transfer screening* to determine where to target further investigations,
- *knowledge acquisition* to construct new profiles for use during screening,
- *knowledge sharing* to disseminate profiles of money laundering activities quickly, reliably, and in a useful form, and

Figure 4-1: How Technologies Relate to Each Other




SOURCE: Office of Technology Assessment, 1995

- *data transformation* to produce data that can be easily screened and analyzed.

Each category of technology is used in the technical options discussed in chapter 7. Screening is used in all options, knowledge acquisition in some, data transformation in most, and knowledge sharing in some of the options. Figure 4-1 shows the relative roles of these technologies in wire transfer analysis systems.

## Wire Transfer Screening

Wire transfer screening is the heart of all options discussed in chapter 7. Technologies for screening wire transfers include knowledge-based systems and link analysis. *Knowledge-based systems* automatically make inferences about wire transfers and other data. Effective use of knowledge-based systems requires effective knowledge acquisition—a way of constructing profiles of money laundering. Effective knowledge acquisition, in turn, requires either human experts who know how to reliably screen wire transfers or a large sample of data that are "labeled" to indicate wire transfers of the sort that should be identified by a working system. *Link analysis* helps identify relationships among individual accounts, people, and organizations. Effective use of link analysis requires a variety of readily available data, some of which provide reliable indicators of money laundering activity.

Some technical options use a knowledge-based system exclusively. Others initially screen all wire transfers using a knowledge-based system and then allow analysts to scrutinize some or all transfers using link analysis. In the latter case, the knowledge-based system can be used to filter transfers-only passing on some transfers to the next stage of analysis-or the knowledge-based system can be used to derive additional data—passing on all transfers along with the additional derived data. The latter use is analogous to one part of the Financial Crimes Enforcement Network (FinCEN) Artificial Intelligence System (FAIS) (see box 4-l).

Banks already use a set of relatively simple systems to screen transactions for illicit conduct. Some of these systems screen currency transactions to identify those which indicate "structuring"-a series of transactions designed to evade current reporting requirements (e.g., five deposits of $3,000 each in a single day). Other systems monitor wire transfers to look for countries or individuals that appear on a list compiled by Treasury's Office of Foreign Assets Control (OFAC). While these systems are quite simple in comparison with the configurations discussed in chapter 7, they are examples of how such systems can be in-

## Box 4-1: The FinCEN Artificial Intelligence System

The FinCEN Artificial Intelligence System (FAIS) is currently used to process and analyze all reports received under the Bank Secrecy Act (BSA).[1] Nearly all (more than 90 percent) of these reports are Currency Transaction Reports (CTRs). The Internal Revenue Service (IRS) Detroit Computer Center and the U.S. Customs Service Data Center collect and store BSA reports; FAIS adds value by linking and evaluating these reports.

FAIS uses three basic types of data. BSA reports—referred to as *transactions—are* used directly. Transactions that can be associated with the same person or business are used to create a new data element called a *subject.* Transactions that can be associated with the same bank account are used to create an element called an *account.* The grouping of transactions into subjects and accounts is accomplished by examining information in the transactions (e.g., name, address, social security number). If these items are sufficiently similar, then two transactions are assumed to belong to the same subject.

These three types of data elements—transactions, subjects, and account—are analyzed by another component of FAIS, a knowledge-based system.[2] FinCEN's knowledge-based system is derived from a system originally developed at the U.S. Customs Service for screening CTRs. The knowledge base from the Customs Artificial Intelligence System (CAIS) was re-engineered to function with FinCEN's system, and is continually updated to reflect changes in money laundering methods. The knowledge-based system component of FAIS is used to evaluate the suspiciousness of transactions, subjects, and accounts. Based on indicators that appear directly within transactions, and on additional indicators calculated from those transactions, FAIS assigns a numeric suspiciousness score to each transaction, subject, and account.

On the basis of these scores and several other criteria, FinCEN analysts select subjects and accounts for further investigation. This investigation is accomplished with the link analysis[2] component of FAIS. Link analysis is used to identify networks of financial activities that help to distinguish between legitimate business activities and money laundering.

FALS uses a variety of commercial hardware and software. The system runs on a 6-processor SparcCenter 2000 server and several SparcStation workstations from Sun Microsystems, Inc. The database component uses an SQL server from Sybase, Inc.; the knowledge-based component uses Nexpert Object from Neuron Data, Inc.; the link analysis component uses NETMAP from ALTA Analytics, Inc. In addition to substantial software development done within these products, some additional parts of FAIS were developed using the language C and using Open Interface from Neuron Data, Inc.

FAIS has been operational since March 1993 and processes approximately 200,000 transactions per week, As of January 1995, 20 million transactions had been entered, linked, and evaluated, resulting in 3 million consolidated subjects and 2.5 million accounts. As of May 1995, the system had generated over 400 investigative support reports corresponding to over $1 billion in potentially laundered funds. FinCEN has received over one hundred feedback forms from outside agencies, as well as internal feedback. Over 90 percent of the feedback indicates either new cases opened or relevance to ongoing investigations.

---

[1] For additlonal description of FinCEN, see chapter 3

[2] See main text for an explanation of knowledge-based systems and link analysis

SOURCES: Ted Senator, Financial Crimes Enforcement Network, personal communications, March 1994- June 1995. U.S. Treasury, Financial Crimes Enforcement Network, "FinCEN Artificial Intelligence System. Fact Sheet, " no date Ted Senator, Henry Goldberg, Jerry Wooton, Matthew Cottini, A.F. Umar Khan, Christina Klinger, Winston Llamas, Michael Marrone, and Raphael Wong, "The FinCEN Artificial Intelligence System: Identifying Potential Money Laundering from Reports of Large Cash Transactions," *Proceedings of the 7th Conference on Innovative Applications in Artificial Intelligence, 1995* (forthcoming)

## BOX 4-2: Current Monitoring and Compliance Systems

Some banks and wire transfer systems already have systems that examine currency and wire transactions. These systems are substantially less sophisticated than some proposed systems for wire transfer monitoring. However, they help indicate the state of current bank systems and the environment within which new systems would operate.

**Currency Transaction Reporting**

As noted in box 1-3, Currency Transaction Reports (CTRs) are filed when a customer deposits over $10,000 in cash. However, banks also look for evidence of *structuring—a* series of smaller cash transactions that are intended to evade reporting requirements. Even though these deposits are under the $10,000 threshold, they should be reported because they may indicate money laundering.

Banks and commercial software vendors have developed systems that aggregate multiple currency deposits over specific periods (usually days or weeks). For example, Chase Manhattan Bank, NA, a large money center bank, uses a system that aggregates multiple currency transactions that occur on the same business day. While the activity listed on the system's reports is very low, about 65 percent of Chase Manhattan's Criminal Referral Forms (CRFs) are a direct result of investigating account activity highlighted by the system. Similarly, Atchley Systems, Inc., a commercial software vendor, has developed a system that allows banks to aggregate currency transactions over a fixed specified number of days and report all aggregations that exceed a specific threshold, The system can also flag individual accounts and automatically generate reports on their cash activities each day, The latter component is used when bank managers wish to monitor the cash activity of certain accounts, even though it may not exceed specific thresholds.

**Foreign Assets Control**

Banks are required to comply with regulations issued by the Treasury Department's Office of Foreign Assets Control (OFAC). The regulations were promulgated under SIX statutes that prohibit, in various ways, trade with specific countries, including Cuba, North Korea, Libya, Iraq, Yugoslavia, UNITA (Angola), and Iran. In addition, Executive Order 12947 prohibits transactions with terrorists. To assist banks with compliance, OFAC maintains a list of specially designated nationals (SDNs) and blocked persons that contains over 2,500 entries. Each entry is an individual (e.g., Manuel Noriega) or organization (e.g., Hizballah). For individuals, addresses and titles are sometimes given; for organizations, a list of aliases and address information is generally given. In some cases, separate entries are made for alternative spellings or addresses of individuals or organizations. Each entry also contains a designation of what provision resulted in their inclusion in the list.

tegrated with bank operations and of the challenges posed by such integration (see box 4-2).

### *Knowledge-Based systems*

Knowledge-based systems, often called "expert systems," are computer programs that process data in ways that emulate human experts. They differ from conventional algorithms in several ways. First, the knowledge that is embedded within the system is largely separate from the reasoning methods used to operate on that knowledge. Second, they often are designed so that they can display the path of evidence and facts used to reach a particular conclusion—in essence, knowledge-based systems can "explain" the inferences that they have made.

The knowledge embedded in knowledge-based systems often is expressed in terms of rules of the form shown in figure *4-2.* Rules can directly connect input data to final conclusions; they can begin with intermediate conclusions of other rules; or they can produce intermediate conclusions that

## BOX 4-2: Current Monitoring and Compliance Systems (Cont'd.)

Banks are required by OFAC regulations to block wire transfers going to organizations and individuals on the list. In the past several years, OFAC has imposed millions of dollars in civil penalties involving U.S. banks. Most of the fines were levied because a bank failed to block an illicit transfer that was processed manually (OFAC has not generally penalized banks for failing to block transfers that were processed automatically). Most large U.S. banks have computer systems in place to screen wire transfers. Several dozen banks and vendors have developed systems that automatically screen incoming wire transfers for locations, organization, and persons on the OFAC list. When one or more of these names IS found, the transfer is stopped and brought to the attention of a human operator. The presence of such software is "considered favorably" when OFAC investigates a bank that failed to block an Illegal transfer.

**Fedwire Scanning System**

The Federal Reserve Bank has the capability to electronically scan and retrieve records of wire transfers made over its Fedwire system. The system is useful for fulfilling law enforcement requests for Fedwire transfer records, but the capability is extremely limited in comparison to the systems contemplated in this report. In the past several years it has been used only infrequently.

With an appropriate search warrant, law enforcement agencies can request a search of Fedwire records. Each search can specify up to twenty different character strings; each string can represent a distinct item (e.g., name, account number, street address), different permutations of the same item (e.g., multiple spellings of a name), or a combination of the two. Only exact matches are reported

There are several limitations to the searches. First, searches can cover only records from the past 180 days, Records older than 180 days are transferred to microfiche and must be searched manually. Second, each search can review the records from only one Reserve Bank's Fedwire traffic. If a law enforcement agency is uncertain which Federal Reserve Banks may have processed a desired transfer, it may have to submit multiple requests. Third, searching a single day of Fedwire records takes approximately one hour and searches can only be done during hours when Fedwire is closed and after the end-of-day processing has been completed. Currently, this amounts to only a few hours each night, and this time will be reduced even further when Fedwire expands its hours of operation in 1997.

Despite these limitations, there are reasons that law enforcement agencies might wish to obtain records through Fedwire scanning rather than through records at an individual bank. It may not be known which of the 11,700 banks with access to Fedwire sent or received the transfer. Also, if law enforcement agents believe that bank employees are complicit in money laundering, or that the bank would inform account holders of the records request, then they may wish to obtain the records through Fedwire scanning.

SOURCES: Joyce Goletz, Chase Manhattan, NA, personal communication, Apr. 7, 1995 Jim Atchley, Atchley Systems Inc., personal communication, May 3, 1995 U S Department of Treasury, *Foreign Assets Control Regulations for the Financial Community* April 13, 1995 U.S. Department of Treasury, Off Ice of Foreign Assets Control, *Specially Designated Nationals and Blocked Persons,* April 18, 1995 Louise Roseman, Associate Director, Division of Reserve Bank Operations and Payment Systems, Board of Governors of the Federal Reserve System, personal communication, May 1, 1995 Jo Ann Harris, Assistant Attorney General, Criminal Division, U.S. Department of Justice, Memorandum to All United States Attorneys, January 31, 1994

will be used by other rules. Knowledge-based systerns often employ hundreds or thousands of such rules to emulate expert reasoning within a narrow domain. The collection of rules is referred to as a *knowledge base.*

The knowledge base is the input to an *inference engine,* an algorithm that uses the knowledge base and input data to reach final conclusions that are then provided to the user. The user can query the

Figure 4-2: An Example Rule

| | |
|---|---|
| IF | Destination bank is foreign; and amount is > $300,00; and originator is not a corporation |
| THEN | Wire transfer is suspicious |

SOURCE. Off Ice of Technology Assessment, 1995

knowledge-based system to trace its pattern of reasoning.

The knowledge represented in a system's knowledge base can be acquired in one of two ways. Most commonly, knowledge bases are constructed by interviewing one or more experts in an area in ways that are meant to elicit the details of their reasoning processes. Less frequently, knowledge bases are constructed by analyzing a large number of cases where the correct decision is known. Both of these approaches are covered below.

Knowledge-based systems were developed in the 1970s largely as a result of efforts to construct two major systems: the DENDRAL system for elucidating chemical structures and the MYCIN system for diagnosing and recommending treatment for infectious diseases.[2] Knowledge-based systems are now widely applied in many fields, including industry, government, medicine, and science.[3] They have been applied to a wide variety of problem types, including diagnosis, repair, and scheduling.

### *Link Analysis*

Link analysis is a technique to explore associations among a large number of objects of different types. In the case of money laundering, these objects might include people, bank accounts, businesses, wire transfers, and cash deposits. Exploring relationships among these different objects helps indicate networks of activity, both legal and illegal (see figure *4-3).*

Link analysis can indicate where to focus investigations. For example, if a person is associated with other persons or businesses that are known to be engaged in criminal conduct, then additional investigation of that individual may be warranted. Similarly, link analysis can help to confirm suspicions. For example, there may be ambiguous evidence of criminal activity for a single individual, but if that person is connected with many other persons and businesses that also appear to be involved in criminal conduct, then the analysis offers some confirmation of the initial suspicion.[4]

Link analysis operates on a set of data records, where each record has several *fields* containing information. These might be records of an individual (with fields of name, address, and phone number), bank account (account number, owner, bank), or business (name, owners' names, board members, address). Link analysis looks for matching fields in each of these records. For example, these matching fields could indicate that two persons live at the same address, deposit into the same bank account, or are involved in the same business.

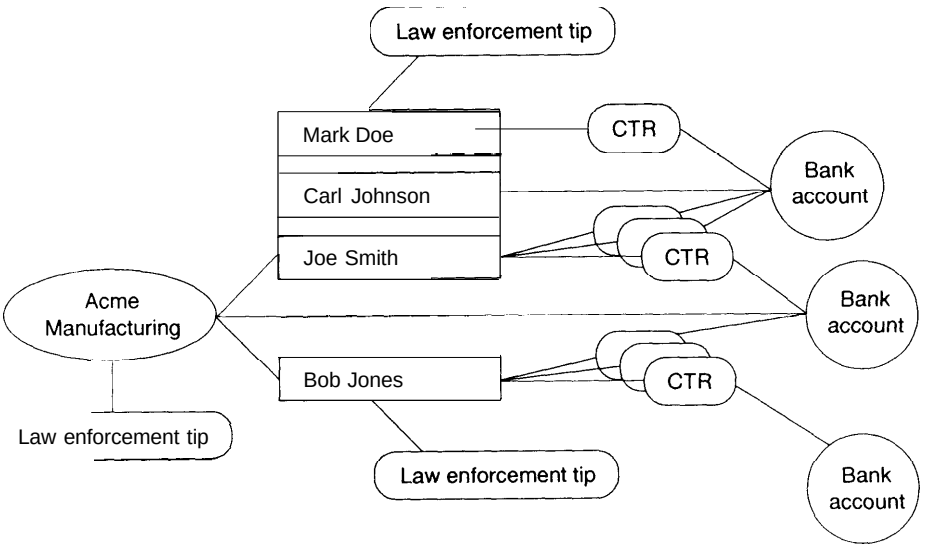
[1] B. G. Buchanan and E. A. Feigenbaum, "DENDRAL and Meta-DENDRAL: Their Applications Dimension, *''Journal of Artificial Intelligence*, 11:5-24, 1978.

[2] B. G. Buchanan and Shortliffe, E. H. (eds.), *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project* (Reading, MA: Addison-Wesley, 1984).

[3] Interested readers should consult the proceedings of a conference on AI applications held annually since 1989: *Innovative Applications of Artificial intelligence* (Menlo Park, CA: AAAI Press; Cambridge, MA: MIT Press).

[4] For additional information, see: Malcolm K. Sparrow, "Network Vulnerabilities and Strategic Intelligence in Law Enforcement," *International Journal of Intelligence and Counterintelligence*, 5(3):255-274.

Figure 4-3: Example of Link Analysis Results




KEY: CTR=Currency Transaction Report

SOURCE Off Ice of Technology Assessment, 1995

Link analysis is a relatively new technique, although it has quickly gained adherents in law enforcement agencies in the United States and elsewhere.[5] The field has its own journal and a professional society,[6] although these are almost entirely oriented to the use of link analysis in social science, not law enforcement. One early promoter and developer of link analysis in law enforcement is Anacapa Sciences, Inc.[7] Because of the prevalence of this company's training, many law enforcement sources refer to link analysis as "Anacapa charting." Link analyses have been used in many criminal investigations, including serial murders, fraud, and conspiracy cases.

Several commercial software packages can be used to conduct link analyses. One popular commercial package for link analysis is NETMAP from Alta Analytics Corporation.[8] NETMAP is used by both FinCEN and the Australian Transaction and Reports Center (AUSTRAC), as a part of systems developed in-house at both agencies. In addition, NETMAP is used by several state agencies investigating financial crimes by analyzing currency transaction data.[9]

[5] Clive Davidson, "What Your Database Hides Away, ''*New Scientist*, January 9, 1993, 28-31. Roger H. Davis, "Social Network Analysis: An Aid in Conspiracy Investigations," *FBI Law Enforcement Journal*, December 1981, pp. 11-19.

[6] *Social Networks* and the International Network of Social Network Analysts, respectively.

[7] Anacapa Sciences, Inc., Santa Barbara, California.

[8] Alta Analytics, Dublin, Ohio. NETMAP is a trademark of Alta Analytics.

[9] Besides NETMAP, there are at least three other software packages for link analysis: Criminal Network Analysis (Anacapa Sciences, Inc., Santa Barbara, California); Watson (Harlequin Group, Ltd., Boston, Massachusetts (U.S. Office)); Analyst's Workbench (12, England). In addition, Syfact (Inter Access Consultancy B. V., Hilversum, The Netherlands) is a specialized package that uses link analysis to search financial data for indicators of money laundering and fraud.

Link analysis is useful for money laundering investigations mostly because it can integrate many different sources of information. The individual records that FinCEN currently receives, and the records that might be available under wire transfer monitoring proposals, provide few indicators of suspiciousness. Link analysis provides a way of combining these different records so that patterns of illegal activities can be discovered. While other methods can supplement it, link analysis may be the only method of analysis that allows these records to be used productively.

Link analysis is a useful way of discovering and displaying links between objects,[10] but it does not automatically construct meaning from those links. That task is left to the analyst. In the case of money laundering, analysts must make judgments about whether a network of links represents a legitimate pattern of personal and business associations, or whether the network represents a criminal organization. Links to database records that show prior criminal activity or suspicious activities (e.g., criminal referrals, suspicious transaction reports, etc.) can aid these judgments.

Link analysis is computationally intensive. Constructing links involves determining whether objects share common data values (e.g., whether a person and a business both share the same address). Consequently, rather than merely examining each record, the analysis must examine each possible pair of records, although some shortcuts can be used to reduce the necessary computation.

Even with these difficulties, however, practical limits on analysis are not unduly restrictive. Using available software and workstations, it is possible to run analyses with tens of thousands of objects. Analyses with hundreds of thousands of objects, however, exceed the capacity of available software and hardware. This indicates that wire transfer data (currently generated at a rate of nearly three million records per day) would have to be segmented or aggregated before it is combined with additional data and analyzed.

### *Other Techniques*

In addition to the relatively sophisticated analysis provided by knowledge-based systems and link analysis, several simpler techniques are useful for screening. For example, FinCEN's FAIS computes statistics based on Currency Transaction Reports (CTRs) and other reports received by the agency. FAIS uses the value of these statistics (e.g., number of CTRs filed in past year, number of suspicious transaction reports filed in past year) to evaluate the suspiciousness of individual subjects and accounts. These statistics are a simple, but relatively powerful, way to evaluate financial records for evidence of money laundering.

## Knowledge Acquisition

As previously noted, knowledge-based systems require a *knowledge base*—knowledge about money laundering encoded in ways that the system can use to make inferences. Knowledge bases can be constructed in two ways: by interviewing an expert (often called knowledge engineering) or by analyzing a large number of cases (often called knowledge discovery or data mining).

Knowledge engineering attempts to capture the relevant heuristics, or "rules of thumb," used by experts to reach conclusions in the relevant domain (e.g., wire transfers and money laundering). Knowledge engineering can be difficult, because experts often cannot easily articulate their decisionmaking processes within the narrow language used by knowledge-based systems. In addition, experts sometimes rely on broad "common sense" knowledge in order to draw useful conclusions, making the knowledge engineering task unreasonably large.

[10] The terminology used here ("objects" and "links") is not universal. Some law enforcement agencies refer to "entities" and "relationships"; the mathematical field of graph theory refers to "vertices" and "edges."

Figure 4-4: Example Data Set

| Money laundering? | Dollar amount | Foreign beneficiary? | Customer type | ... |
|---|---|---|---|---|
| No | 110,000 | Yes | Foreign exchange | ... |
| No | 3.5 million | No | Industrial | ... |
| No | 243,032 | Yes | Retail | ... |
| No | 322 | No | Individual | ... |
| No | 87,436 | No | Bank | ... |
| ... | ... | | ... | ... |
| Yes | 574,945 | Yes | Retail | |
| ... | ... | ... | ... | ... |

SOURCE Off Ice of Technology Assessment, 1995

Knowledge engineering in the area of wire transfers is only possible if there are people who know how to screen transfers for evidence of money laundering. There are no human experts who scan large numbers of wire transfers and reliably distinguish between legitimate and illegitimate wire transfers. Consequently, knowledge engineering techniques are of little help in building a wire transfer monitoring system. Instead, knowledge discovery techniques must be employed.

Knowledge discovery techniques are diverse and multifaceted, including techniques from statistics and the AI subfield of machine learning. In addition, an emerging set of data visualization techniques are also gaining recognition. Several knowledge discovery techniques have been proposed for use at FinCEN, but none are now used. The boundary between screening and knowledge discovery is not a clear one, and techniques currently in use (e.g., link analysis) can be used to identify new patterns. Some knowledge discovery techniques are only useful when there are a large number of cases where the answer is known-that is, whether the wire transfer (or person, account, etc.) can be labeled as involved with money laundering or not.[11] Other knowledge discovery techniques can be somewhat useful even in the absence of such clear labels.

## Machine Learning and Statistical Model Building

Researchers have developed several techniques in the past few decades for automatically finding patterns in large amounts of data. In most cases, the data consist of a large number of *observations*, where each observation represents a single object (e.g., a person, account, or wire transfer) and consists of values for each of several numeric or symbolic variables. A fragment of a fictitious data set is shown in figure 4-4.

Analysis begins by designating one variable (e.g. “Money Laundering?” in figure 4-4) as the

[11] Similarly, link analysis is only effective if some indicators of criminal activity are available. Without evidence that at least some of the objects (e.g., individuals, accounts, businesses) are inherently suspicious, it will be difficult to distinguish between legitimate and illegitimate patterns of activity. If such indicators are not present, or are not present in sufficient number, interpreting link analysis results requires an additional step--determining what patterns of associations indicate money laundering.

variable of interest.[12] The rest of the analysis consists of deriving *models* that attempt to accurately predict this variable by using the remaining variables (e.g., dollar amount, foreign beneficiary, customer type, and others in the example above). Models can be in the form of algebraic equations, logical rules, weighted networks,[13] or any other way of relating the values of one or more variables to the value of another variable.

Models are usually derived by a process of searching through large numbers of possible models. Each possible model may use different sets of variables or combine the same variables in different ways. Models that accurately predict the variable of interest are retained, while less accurate models are discarded. In many cases, it is not feasible to search through all possible models,[14] so techniques often limit the number of models searched by selectively altering the most accurate models that have already been constructed.

Technologies for machine learning and statistical model-building have existed for at least three decades, but they continue to be an active research area.[15] Interest in analysis of large databases has grown tremendously in the past five years, as major corporations have begun to "mine" large databases of customer information. This has spurred interest in massively parallel computing hardware, new algorithms for model construction, and new model forms.

### *Clustering*

Researchers in both statistics and AI have developed methods of looking for closely related groups of objects. Cluster analysis can be used to determine underlying groupings that are not otherwise apparent in the data. For example, cluster analysis of wire transfers could be based on the frequency and dollar amount of each transfer, as well as the type of beneficiary. Such analysis could reveal groups of transfers whose originators are highly similar (e.g., brokerage houses, industrial firms, or money transmitters).

Computational techniques for cluster analysis partition a set of observations into groups based on one or more variables (e.g., frequency and dollar volume). The ultimate goal is to produce groups that differ greatly in terms of one or more variables, but where the individual members of each group differ little in terms of those variables. Figure 4-5 is an example of a graph showing several clusters in terms of two variables.

In financial data, clusters might reveal similar types of accounts, individuals, or organizations. For example, the currency and wire transactions of manufacturing firms might cluster closely together in comparison to other firms. Similarly, insurance companies might resemble each other closely in terms of their financial transactions. These clusterings might allow investigators to identify manufacturing firms whose financial transactions are atypical and examine them more closely to determine whether the corporation is merely a "shell" within which to conceal money laundering.

### *Visualization*

Visualization techniques use color and interactive graphics to allow users to explore the relationships among two or more variables. Rather than automating the construction of useful models like machine learning techniques, visualization tech-

---

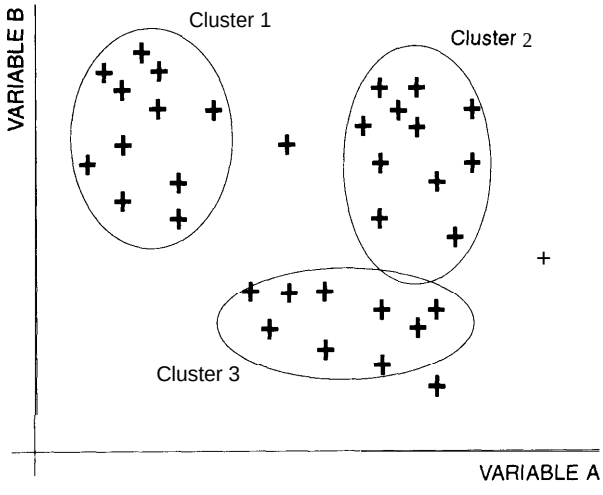
[12] Some techniques do not require designation of a specific variable of interest. An example is cluster analysis, a method that searches for groupings of observations that are all highly similar (see section below). These techniques can help an analyst understand a data set, but they do not directly help construct predictive profiles.

[13] This approach is described in more detail in a later section.

[14] Some methods do search all possible models within a limited range, but they are relatively rare.

[15] Interested readers can consult the proceedings of three groups of workshops and conferences: Machine Learning (held annually since the mid-1980s), Knowledge Discovery in Databases (held periodically since 1989), and Artificial Intelligence and Statistics (held biennially since 1985). Another source is articles in the journal *Machine Learning* (Hingham, MA: Kluwer Academic Publishers).

Figure 4-5: Example of Clustering




SOURCE: Office of Technology Assessment, 1995

niques give human analysts powerful tools to examine data—allowing analysts to explore and apply their own knowledge to the data analysis problem.[16] In addition, visualization techniques allow analysts to apply their own abilities to recognize patterns in data, a human ability that machines cannot yet duplicate.

## Other Techniques

Several other technologies are difficult to classify as either screening or data analysis, but they are potentially relevant to the problem of wire transfer analysis. Case-based reasoning and neural network technologies can be used both to derive profiles from data and to help apply those profiles.

Case-based reasoning techniques rely on the storage and processing of prototypical cases (i.e., observations), rather than deriving an abstract profile based on the values of particular variables. For example, a case-based reasoning approach to profiling wire transfer data might involve selecting records (e.g., wire transfers, CTRs, criminal referrals) that are prototypical of different classes of legitimate traffic, as well as selecting records that are prototypical of different types of illegitimate traffic (e.g., multiple cash deposits under $10,000 in a single day). These prototypical cases would then be compared to new records—helping to determine what type of activity they represent.

Neural network techniques attempt to emulate the information processing of biological networks of neurons, one of the fundamental structures of the brain. Neural networks are a set of interconnected elements called *nodes.* Some nodes are inputs and take on the values of particular variables (e.g., amount of transfer); other nodes are outputs and are used to determine the answer suggested by a network (e.g., whether a wire transfer is suspicious). Many networks also have internal, or "hidden," nodes. Nodes are interconnected and each connection has a weight, indicating the strength of the influence of the value of one node on the value of another.

By adjusting the weights on each connection, neural networks can be made to produce nearly any output based on a given set of inputs. Given a set of data where each observation contains a set of inputs (e.g., amount of transfer, foreign beneficiary, etc.) and a known output (e.g., suspiciousness), the network can be trained to implicitly recognize patterns in the input, if such patterns are present. However, one potential disadvantage of neural networks in the context of wire transfer monitoring is that they can make it difficult or impossible to "explain" why a particular transfer (or person, account, etc.) was identified as suspicious. Neural networks differ from many knowledge-based systems in this regard, because the knowledge represented within the network is not explicit or intelligible. This characteristic would cause difficulties if the results of the network's analysis needed to be explained to law enforcement agents, judges, or juries.

[16] Link analysis can be thought of as a visualization technique. Chris Westphal and Bob Beckman, "Data Visualization for Financial Crimes and Money Laundering Investigations," *Proceedings of the ONDCP/CTAC International Symposium on Tactical and Wide-Area Surveillance,* Chicago, IL, 1993.

## Knowledge Sharing

Several of the technical options for wire transfer monitoring require that knowledge-based systems be installed at multiple locations. Some configurations require installation at wire transfer systems (e.g., CHIPS and Fedwire); others require installation at large money center banks, and still others require installation at many or all banks.[17]

Locating knowledge-based systems at several locations poses a unique challenge in terms of updating and maintaining the knowledge base of those systems. Because money laundering techniques can change rapidly, the profiles in knowledge-based systems intended to detect money laundering would have to change as well. Updating multiple screening systems could be done in three ways. First, all banks and wire transfer systems could be required to use a standard software package supplied by regulatory agencies. Such an approach would simplify updating but would also impose regulatory burdens, limit flexibility, and discourage innovation. Second, banks and wire transfer systems could be provided with textual descriptions of new profiles, allowing them to alter their monitoring systems appropriately. This approach would impose little burden on the federal government but would require each bank and/or wire transfer systems to recode their monitoring systems, perhaps causing long delays in the use of the profiles. Finally, banks and wire transfer systems could be provided with the profiles in a way that would facilitate updating multiple, heterogeneous knowledge-based systems.[18]

Some initial research on this latter option, referred to as *knowledge sharing*, has been conducted in the last five years. Much of the research has been conducted under the Knowledge-Sharing Effort, a project sponsored jointly by the Air Force Office of Scientific Research, the Defense Advanced Research Projects Agency, the Corporation for National Research Initiatives, and the National Science Foundation.[19] Research on knowledge sharing includes techniques to translate between different languages for encoding knowledge bases, to remove arbitrary differences between such languages, to create a standard protocol for knowledge-based systems to communicate, and to develop generic and reusable knowledge bases.

Although the research is progressing, knowledge sharing techniques are not well-developed and are substantially less mature than many of the other techniques discussed in this chapter. However, wire transfer monitoring poses only relatively small challenges to knowledge sharing. The knowledge bases that are shared are likely to be relatively small. The complexity of the domain is relatively low, given that wire transfers have a small number of fields and that wire transfer screening systems (outside of FinCEN) are likely to employ only small amounts of additional data. Finally, the use of knowledge sharing techniques can easily be phased-in over a period of time, starting with communicating profiles using relatively standard terminology, and perhaps moving toward electronic dissemination of specially formatted knowledge bases.

## Data Transformation

Data transformation issues are some of the most troubling and time consuming aspects of analyzing financial records (e.g., CTRs) and experience indicates that wire transfer data are likely to present at least as many problems. For example, determining whether two different transfers originated from the same individual is not easy. Financial re-

[17] This latter possibility could involve an extremely large number of systems. There are approximately 11,500 commercial banks in the United States.

[18] All of these options would disseminate law enforcement profiles of money laundering and would pose a risk of these profiles falling into the hands of money launderers. This concern is discussed briefly later in this chapter.

[19] Robert Neches, Richard Fikes, Tim Finin, Tom Gruber, Ramesh Patil, Ted Senator, and William R. Swartout., "Enabling Technology for Knowledge Sharing," *AI Magazine*, Fall 1991, 12(3): 36-56.

cords do not always contain unambiguous indicators such as a social security number; small variations in format and spelling can defeat simple word matching; addresses are not typically provided and frequently change;[20] money launderers can use multiple, shifting account numbers. As a result, FinCEN and AUSTRAC have explored and implemented various schemes to process textual information to allow matching of names and addresses of institutions and individuals. In addition, AUSTRAC uses some approaches to understanding written text, referred to as *natural language processing*, in order to glean additional information from free text fields of wire transfers.

Other sorts of data transformations involve producing new records from existing ones. For example, FinCEN's FAIS produces new records for individual persons and accounts by aggregating data from CTRs and other reports. Fields in these records are then filled with data calculated using various statistics (e.g., number of CTRs marked as "suspicious," total cash deposits).

Both FinCEN and AUSTRAC use a database that contains both original data records (e.g., CTRs) and records constructed by the system itself (e.g., a record representing an account, constructed by aggregating a number of CTRs). This concept of a database containing both original and constructed records is nearly identical to an AI-based concept referred to as a *blackboard*.[21] A blackboard is a central database where multiple problem-solving agents can share related information about a particular problem over a period of time.[22] In the case of wire transfer analysis, the "agents" may be banks that report wire transfers, conventional computer systems that create aggregated records, knowledge-based systems that enhance or create records, or human analysts who enhance or create records.

A blackboard architecture can allow continuous enhancement and development of knowledge about potential money laundering cases over days, weeks, or months. In theory, the knowledge about those cases can be updated and developed by different analysts whose only communication is through the blackboard. In fact, many law enforcement databases can be thought of as blackboards. Agents enter reports that are used by later investigators without the need for direct communication between them even though they are geographically separated or separated in time.

## DETECTING MONEY LAUNDERING

Before examining the applicability of different technologies, it is important to examine the task of detecting money laundering activity in wire transfer data. This section discusses wire transfer data, other types of data that might be combined with it, and characteristics of profiles that might be developed.

### Wire Transfer Data

Wire transfers contain three basic categories of information: 1) information on the originator (name, address, account number, bank, routing number); 2) information on the beneficiary (name, account number, bank, routing number); and 3) information about the transfer itself (dollar amount, date, payment instructions, intermediary banks, internal codes).

Analyzing the relatively small amount of data in each transfer presents a surprising array of problems. These problems include the extremely large

---

[20] Addresses and other information will be mandatory under new Treasury Department regulations, although money launderers could evade these requirements by providing false, flawed, or misleading information.

[21] Ted Senator, Henry Goldberg, Jerry Wooton, Matthew Cottini, A.F. Umar Khan, Christina Klinger, Winston Llamas, Michael Marrone, and Raphael Wong, "The FinCEN Artificial Intelligence System: Identifying Potential Money Laundering from Reports of Large Cash Transactions," *Proceedings of the 7th Conference on Innovative Applications in Artificial Intelligence*, 1995 (forthcoming).

[22] A blackboard architecture was first constructed in the HEARSAY speech understanding system. L. Erman, F. Hayes-Roth, V. Lesser, and D. Reddy, "The HEARSAY II Speech Understanding System: Integrating Knowledge To Resolve Uncertainty," *Computing Surveys*, 12(2): 213-253, 1980.

number of transfers, incomplete or faulty data, heterogeneous formats and recordkeeping systems, and other difficulties for supplying cases for data analysis.

### *Large Volume of Data*

U.S. wire transfer systems handle hundreds of thousands of transactions per day. Taken together, CHIPS, SWIFT, and Fedwire handle some 700,000 transactions in the United States each business day. This volume of data dwarfs the Bank Secrecy Act data, some 30,000 reports per day, that are currently received, processed, and analyzed at FinCEN.

Although the number of wire transfers is large when compared to financial reports currently filed with FinCEN, the size of each transfer message is quite small. For example, the current format for a Fedwire transfer is limited to 600 characters. Even the expanded Fedwire format, due to be used in 1997, will use a maximum of 1,700 characters. Wire transfers rarely use all the available characters; wire transfers in both Fedwire and CHIPS average about 300 characters in size.[23] In comparison, CTRs currently collected and analyzed at FinCEN average around 1,000 characters.[24]

The volume of reporting to FinCEN is of particular concern, given past experience with CTR reporting. Until mid-1993, the volume of CTRs far outstripped any ability to analyze and monitor them. Now the FinCEN AI System analyzes every CTR at least once, but banking industry representatives still charge that many CTRs are relatively useless and do little but impose reporting costs on banks. These concerns are behind the recent revision to the CTR reporting requirements designed to reduce the volume of these reports filed by banks. A broad reporting requirement for wire transfers could raise similar objections, but on a far greater scale.

As is the case with CTRs, many wire transfers could be excluded from required reporting by using relatively simple criteria. AUSTRAC uses exclusions to reduce the volume of wire transfer data delivered to the agency, and similar exclusions could be used in the United States.

Clearly, there is some risk to excluding broad categories of wire transfers from reporting requirements. Money launderers could attempt to make their wire transfers fall into the categories excluded from reporting. Reporting exclusions would have to take this risk into account and only exclude categories of transfers that could not easily be used by money launderers. For example, some wire transfers by banks aggregate many smaller transactions. These transfers carry little or no information about the original transactions and could be excluded on the assumption that only regulatory scrutiny could uncover money laundering by banks.

### *Data Transmission, Processing and Storage*

Some of the technology configurations identified by OTA involve the transmission of wire transfer records from banks to FinCEN. Electronic transmission of CTRs by banks to the Internal Revenue Service (IRS) or Customs data centers is increasing, but the addition of wire transfer records could swell the volume of these electronic records by a factor of 10 to 100. The mere transmission of these data would strain current networks, and storage and analysis of these records might be beyond the capacity of current technology. A critical question then becomes whether the number of transfers transmitted might be reduced, either by exempting classes of funds transfers or by requiring banks to commit some preliminary processing of the transfers.

The security of funds transfer information is another issue, both as the information is transmitted and as it is stored. These records, if leaked or stolen, could help competitors identify a company's suppliers and customers, detail its cost structure, or predict its future behavior. Encryp-

[23] Mike Rosenberg, Senior Intelligence Research Specialist, FinCEN, personal communication, February 1995.

[24] Ted Senator, Chief, Systems Development Division, FinCEN, personal communication, February 1995.

tion suggests one manner of ensuring secure transmission, but securing the information at the federal repository is not a simple matter.[25]

There is no centralized database of wire transfers. Depending on the origin and destination of a wire transfer, messages making that transfer may flow over one or more of the three major systems (CHIPS, SWIFT, and Fedwire). Even individual wire transfer systems do not always maintain centralized databases of the transfers traveling through their system. For example, Fedwire data are decentralized in three different locations (although that will shrink to two locations by the end of 1995).

In addition, not all data are kept in a form that is easily accessed. For example, the Federal Reserve (Fedwire) keeps records online for three days, on tape for six months, and on microfiche for seven years. Bank records, although they originate in electronic form, are often stored electronically for only a short time. Some large banks keep long-term records on microfiche and some small banks keep records on paper, although banks are increasingly moving toward electronic storage. In addition, even electronic data are not always easily retrievable. For example, Fedwire data are currently indexed by sending and receiving bank only. Other fields (e.g., recipient account) may be located by using a search program to look for strings of characters, but even a relatively small number of requests (e.g., a few requests for use of the program per day) would be extremely demanding on the current system. See box 4-2 for details on the Fedwire scanning system.

The various recordkeeping and computer systems used to conduct and record wire transfers were not intended for the activities contemplated in monitoring proposals. They were intended to quickly and reliably process a large volume of wire transfers. This mission does not require centralized recordkeeping, long-term electronic storage, or quick retrieval of the sort required for law enforcement purposes. It is certainly possible to construct a system that would allow decentralized storage and retrieval of data.[26] However, it would substantially complicate wire transfer analysis and it would impose substantial new costs on banks and/or wire transfer systems.

### *Incomplete or Faulty Data*

Some wire transfers contain blank fields or relatively useless information. Accurate information in these fields are not required for the transfer of funds, although they would be useful for law enforcement purposes. For example, some foreign banks refuse to reveal the name of the originator of a wire transfer, saying only that the transfer originates from "our good customer." Even where information is required, individuals or organizations wishing to confound analysis could provide false or misleading information.

In addition, wire transfer data sometimes contain errors. In some cases, these errors are mistakes or typographic errors made at the bank level. In other cases, the errors result from operators who use fields in ways that were not originally intended when the format of wire transfers was

[25] For example, see U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994).

[26] An example of such a system is NASA's Earth Observing System Data and Information System (EOSDIS). See Office of Technology Assessment, U.S. Congress, *Remotely Sensed Data: Technology, Management, and Markets* (Washington, DC: U.S. Government Printing Office), September, 1994.

created.[27] Occasionally, messages are returned and resent in order to correct errors in the original transmission, and this procedure could complicate simple data analysis schemes that assume each transfer of funds is only associated with a single wire transfer record.

An additional problem is created by variations in individual and business names and addresses. Many of the fields in wire transfers (e.g., originator name, beneficiary name) are entered as free form text. These fields are subject to format differences (e.g., ACME, Inc.; Acme, Incorporated, ACME Corporation; American Consolidated Mining and Engineering, Ltd.) and misspellings. These can make it difficult to identify wire transfers that correspond to the same individual or business. Additional fields, such as address and account number, can be used, but individuals and businesses can operate multiple accounts and use several addresses.[28]

### *Heterogeneous Data Formats and Data Types*

Wire transfers vary greatly in their characteristics. For example, different classes of banks typically make different types of transfers and there are several different wire transfer systems, each with its own format. This produces wide variability in transfer records.

Money laundering analysts emphasize that many different types of entities (e.g., transfers, individuals, accounts, companies) would need to be handled by any comprehensive analysis system. Money laundering profiles developed by law enforcement and regulatory personnel involve relationships among these different entities, rather than the properties or behavior of a single entity.

### *Fragmentary Records*

One approach to detecting money laundering would be to compare the behavior of individuals and companies to general profiles of behavior for types of individuals and companies. For example, the behavior of an individual could be compared to the behavior of others in his or her socioeconomic group. Many fraud detection systems in the credit card, cellular communications, and health care fields rely on this approach (see box 4-3).

However, these fraud detection systems have a distinct advantage—credit and cellular communications companies have relatively complete records of each individual customer, and health insurance companies have relatively complete records of each health care provider. Merely by virtue of doing business with the company, customers and health care providers must supply basic information. In addition, because transaction records are clearly designated as belonging to a particular customer, companies can construct detailed profiles of the customer's typical patterns.

In contrast, FinCEN has only fragmentary records on the individuals and companies that it investigates, and wire transfers offer little improvement in this regard. Social security numbers are not provided on wire transfers, so linking together multiple transactions would require much more effort. Much of the FinCEN AI system is devoted to accurately aggregating Bank Secrecy Act (BSA) data to form records of accounts and individuals by using inexact identifiers such as name and address. Even after this aggregation is accomplished, the resulting records form only a

---

[27] Because of problems with anomolies and errors in wire transfer messages, specific software has been designed to correct errors in some message types. For example, see: Peter Johnson, Joseph Devlin, Stephen Mott, and Jean Jans, "Applying Natural Language Understanding Technology to Automate Financial Message Processing," *Intelligent Information Access,* Proceedings of the BANKAI Workshop, Brussels, Belgium 14-16 October, 1991. Society for Worldwide Interbank Financial Telecommunication S.C. (Editors). Amsterdam: Elsevier Science Publishers, 1992.

[28] As a result of all these problems, according to the American Bankers Association (ABA), some wire messages (such as those associated with bank trust and securities) are often ambiguous enough to confuse trained and experienced human readers. ABA Comments on OTA draft material, received March 24, 1995.

## BOX 4-3: Electronic Fraud Detection at the Travelers Insurance Company

Fraud is a substantial problem for insurance companies. The National Health Care Antifraud Association (NHCAA) estimates that 10 percent of all healthcare claims contain some element of fraud. Such fraud is costly to insurance companies, and they have taken steps to detect and investigate potential fraud cases.

The Electronic Fraud Detection (EFD) system assists fraud investigators at The Travelers Insurance Companies in the detection and preinvestigative analysis of health care provider fraud. The system has many similarities to proposed systems to monitor wire transfers, as well as some Important differences.

In the past, fraud detection has relied upon manual inspection of claim forms and tips from internal sources, law enforcement agencies, and a telephone hotline. However, increasing use of electronic records has made automated analysis possible and has removed the possibilities of some conventional forms of fraud detection (e. g., examining paper claim forms for signs of alteration, etc.). As a result, The Travelers Insurance Companies undertook the development of EFD, a system to detect fraud using automated analysis.

Two of the challenges faced in development of EFD directly mirror problems in developing a wire transfer system. First, the company had no experts with experience screening large numbers of claim forms, The company had experts in claims processing and experts in investigating fraud, but no individuals with experience in the specific task to be addressed by EFD, Second, current data were insufficient to develop a system. The known cases of fraud were judged to be inadequate for statistical or machine learning approaches. Both problems were cited by the developers as major barriers to developing EFD.

Despite these difficulties, a system was developed that relies upon assembling a detailed statistical profile of each healthcare provider and then comparing that profile to other providers of the same type. Since each provider files a large number of claim forms, statistics can be derived, indicating the number of services of a particular type and the number of services of an unexpected type performed by a given provider. These statistics can then be compared with averages for comparable providers. For example, the statistics of a particular chiropractor can be compared to all chiropractors in the same City.

Potential fraud cases are Identified when a provider differs from other providers in ways that are both statistically significant and indicative of fraud. The system uses heuristics or “rules of thumb” that indicate why a particular statistic is indicative of fraud, and what sort of deviations from average are important. For example, some statistics may not be indicative of fraud if they are lower than normal, but only if they are higher than normal.

EFD demonstrates that it is sometimes possible to construct a system where no expert and few data exist. However, there are important differences between health care fraud detection and wire transfer analysis. First, The Travelers has detailed information available on each healthcare provider because providers file a large number of claims each year. Data from wire transfers and CTRs are likely to be fewer and more fragmentary.

Second, based on the NHCAA estimate, 10 percent of all health care claims involve some fraud. In contrast, probably around 0.05 percent of all wire transfers involve money laundering. This poses a much greater challenge, since without high accuracy, an automated monitoring system would produce an unacceptably large number of false positives.

SOURCE John A Major and Dan R Riedinger, “EFD: A Hybrid Knowledge/Statistical-Based System for the Detection of Fraud, ” *International Journal of Intelligent Systems, 7 687-703, 1992*

fragmentary record of the individual or account in question.

### *Difficulties With Supplying Cases of Money Laundering for Data Analysis*

It is difficult to label individual transfers, persons, accounts, or businesses as definitely associated with money laundering within the time frame relevant to crime detection. Years often elapse between the time that wire transfer records are generated and the conclusion of a law enforcement investigation of relevant leads or suspects. Even if criminal prosecution records were carefully matched with wire transfers, it is unlikely that concluded cases would identify all, or even most, of the records that were actually involved with money laundering. Law enforcement agencies clearly do not identify or prosecute all money laundering activity and may catch only the incompetent money launderers. Thus, by looking at any set of wire transfers, it is not possible to confidently label each as licit or illicit.

Fraud detection systems for credit cards, telephones, and health care do not suffer from this problem to the same extent. Much fraud is "self-revealing"—clearly detectable after the fact. For example, some cellular telephone fraud schemes involve "cloning" the phone of a customer with no involvement in the fraud scheme, and the customer will usually report the fraudulent toll calls when he or she receives a bill.[29]

While this self-revealing characteristic usually does not allow the fraud to be detected as it is occurring, it does provide investigators with a base of positive cases from which to derive overall patterns of fraud. Unfortunately, money laundering almost never is self-revealing. Investigators can only make inferences based on the schemes that they have caught themselves—leaving open the possibility that many other schemes may go undetected.

If imperfectly labeled data about money laundering are used in knowledge acquisition, the resulting profiles may do little more than confirm known methods. Suppose a set of data is labeled so that each known case of money laundering is used as a positive example and all the remaining cases are used as negative examples. The negative examples almost certainly contain undetected cases of money laundering, perhaps representing as many (or more) cases than are being used as positive examples. If these data are used to derive profiles of money laundering, the profiles will be "trained" to ignore negative examples—even though they may, in truth, involve money laundering. The resulting profiles will faithfully profile known money laundering schemes, rather than detect new ones.[30]

This labeling problem impairs data analysis techniques that might be used to construct profiles directly from data using techniques of statistics, machine learning, and visualization.

## Additional Data

Wire transfer data don't exist in a vacuum. There are other types of data that can be used to identify money laundering. In fact, FinCEN currently uses a large number of databases to identify and analyze financial crimes. Table 4-1 details some of the types of information and the specific databases from which it is gathered.

FinCEN information comes from three basic sources: 1) the U.S. Treasury's Financial Database that contains CTRs, Currency and Monetary Instruments Reports, Casino Reports, and Foreign Bank Account Reports; 2) several databases

[29] Not all fraud is self-revealing. For example, some health care schemes involve creating entirely fictitious identities or involve the willing collusion of policyholders. See: Malcolm Sparrow, "The State of the Fraud Control Game; and the Impact of Electronic Claims Processing on Fraud and Fraud Control," Unpublished paper for the 1994 International Symposium on Criminal Justice Information Systems and Technology, 1994.

[30] Malcolm Sparrow, "The State of the Fraud Control Game; and the Impact of Electronic Claims Processing on Fraud and Fraud Control," Unpublished paper for the 1994 International Symposium on Criminal Justice Information Systems and Technology, 1994.

TABLE 4-1: Data Accessible to FinCEN

| Category | Type | Selected specific databases |
|---|---|---|
| Persons | Name; address; former addresses; phone numbers; social security number; legal filings; criminal referrals; large cash transactions; foreign bank account holdings; travel records | Credit bureaus; news reports; U.S. Postal and commercial change of address; missing children database; phone directories; law enforcement and treasury databases |
| Businesses | Name; addresses; financial data; names of officers, partners, and agents; legal and regulatory filings | Dun & Bradstreet; Information America |
| Property | Address, sales information | Courthouse records in 11 states |

SOURCE: FinCEN documents, 1995.

of criminal reports including the Drug Enforcement Administrations's Narcotics and Dangerous Drugs Information System, the INTERPOL Case Tracking System, and the United States Postal Inspection Service; and 3) commercial database services from organizations such as Dun & Bradstreet, LEXIS/NEXIS, and credit bureaus.

In addition to these databases of specific information, some useful data may involve general knowledge about money laundering activities. For example, money laundering is generally thought to employ accounts in countries with strong bank secrecy laws.[31] However, information such as this is relevant only in the context of additional information indicating criminal intent. For example, legitimate corporations use offshore bank accounts in countries with strong bank secrecy laws. This activity, in itself, is not a sufficient indicator of money laundering.

## Money Laundering Profiles

Another set of challenges for wire transfer monitoring systems involves basic facts about money laundering and the current state of knowledge about it. These include the extremely low incidence of money laundering, the lack of tested profiles, the existence of temporal and spatial profiles, and the dynamic nature of criminal conduct, the similarity of licit and illicit conduct, and the need for multiple levels of analysis.

### *Extremely Low Incidence*

The dollar volume of money laundering appears large (one estimate is $300 billion per year worldwide), but is small compared to the total volume of money moved over wire transfer systems in the United States (at least $2 trillion per business *day*, ***$500*** trillion per year). Assuming that all money laundering moves through U.S. wire transfer systems, that each transaction moves once via a wire transfer, and that money laundering transactions are the same size as other transactions, then laundered money would account for approximately 0.05 percent of all wire transfers in the United States (see box 4-4).

The low incidence of money laundering wire transfers exacerbates the problem of false positive identifications of money laundering by an automated or semiautomated system. Because the false positive rate is likely to be orders of magnitude greater than the 0.05 percent incidence of money laundering, the ratio of false positives to

[31] In 1989, these countries were: Antigua, Austria, Bahamas, Bahrain, Barbados, Belize, Bermuda, British Virgin Islands, Cayman Islands, Costa Rica, Channel Islands, Gibraltar, Grenada, Hong Kong, Isle of Man, Liberia, Liechtenstein, Luxembourg, Monaco, Republic of Nauru, The Netherlands, The Netherlands Antilles, Panama, Singapore, St. Kitts, St. Vincent, Switzerland, and Turks and Caicos Islands. Mike Harrington and Marcus Glenn, "Methods for Analyzing Wire Transfer Data To Detect Financial Crimes,"MTR-91 -W00057, McLean, VA: MITRE Corporation.

## BOX 4-4: What Percentage of Wire Transfers Involve Money Laundering?

It is possible to obtain rough estimates of the percentage of wire transfers that involve money laundering, based on:

- the known volume of money transferred over wire transfer systems in the United States;
- estimates of the total amount of money laundering; and
- assumptions about how money launderers use wire transfers.

**Volume of wire transfers;** In 1994, Fedwire transferred over $211 trillion and CHIPS transferred over $295 trillion. The volume transferred in and out of the United States through SWIFT messages is not easily estimated, although it is probably of the same order of magnitude as those of Fedwire and CHIPS. However, many SWIFT messages are automatically converted to CHIPS messages, meaning that simply adding the total dollar volumes of the three systems would result in an overestimate, For the purposes of estimation, $500 trillion per year will be used as the total dollars transferred by wire transfers through the United States,

**Total amount of money laundering:** Estimates of worldwide money laundering are $100 billion to $300 billion annually,

**Assumptions and estimates;** If it is assumed that all laundered funds move through the United States, that they are transferred only once, and that money laundering transfers are no larger or smaller than other transfers, then the percentage of all wire transfers that move through the United States and involve money laundering is between 0,02 percent (100 / 500,000) and 0,06 percent (300 / 500,000),

The estimate could be substantially lower if it is assumed that not all laundered funds pass through the United States, or that not all laundered funds that pass through the United States are sent via wire transfers. Similarly, it could be substantially higher if the same laundered money is assumed to be sent via wire transfer multiple times (in order to evade simple detection schemes). Taking both of these factors into account, OTA estimates that the total percentage of wire transfers that involve money laundering is probably less than one-tenth of one percent (0.1 percent) and that a reasonable median estimate is one-twentieth of one percent (0.05 percent). Given the uncertainty regarding the total amount of money laundering, and how money launderers use wire transfers, these estimates should be regarded as preliminary and highly uncertain.

SOURCE Off Ice of Technology Assessment, 1995

true positives (even if all the true positives are captured by the monitoring system) is apt to be extremely high (see box 4-5).

A high false positive rate would diminish law enforcement's confidence in the system's capabilities. The leads produced by any wire transfer monitoring system must compete for the attention of law enforcement agents. Most law enforcement agencies contacted by OTA noted that they had far too few resources to follow up every possible lead. If most leads provided by a system turn out to be false, law enforcement agents are unlikely to use the output of the system in preference to more reliable information sources.

### *Lack of Tested Profiles*

Building traditional knowledge-based systems involves interviewing an expert about a relatively narrow problem area (e.g., diagnosing bacterial diseases) and constructing a computer-based model of the reasoning process of that expert. Law enforcement agents or analysts do not know how to recognize a wire transfer as money laundering. If wire transfers are examined at all, they are examined in the context of an ongoing investigation, due to limits on law enforcement access to wire transfer data.

## BOX 4-5: False Positives

Because most wire transfers are legitimate, an automated wire transfer monitoring system would face a daunting task. If a system merely classified each transfer as "legitimate" or "illegitimate", it would have to pick out a very small number of transfers as illegitimate, while leaving the vast majority of (legitimate) transfers untouched. Any such system will almost certainly make many errors, due to the basic laws of probability.

Assume that a system examines each of 40,000 wire transfers and classifies each as "legitimate" or "illegitimate." Further, assume that the system is reasonably accurate, correctly classifying 95 percent of the transfers (i. e., in only 5 percent of the cases does it classify a transfer as illegitimate when it actually is not, or vice versa). If the incidence of money laundering in wire transfers is 0.05 percent, then only 20 of the 40,000 wire transfers would, in reality, be illegitimate. The system could be expected to correctly classify nearly all of these transfers (19 out of 20, or 95 percent). Of the remaining 39,980 legitimate transfers, most would be correctly classified (37,981 out of 39,980, or 95 percent). However, nearly 2000 of the legitimate transfers (1 ,999 out of 39980, or 5 percent) would be misclassified. The system would identify them as illegitimate even thought they are not. As a result, the group of transfers identified by the system as Illegitimate would consist almost entirely (99 percent) of transfers that are actually legitimate.

Even if the accuracy of the system is nearly perfect, the results are still discouraging. If the system is 99 percent accurate, then all 20 illegitimate transfers would be correctly classified, and 400 legitimate transfers would be misclassified as illegitimate. Therefore, even with a system with remarkable accuracy, nearly all of the transfers identified as illegitimate actually would be legitimate. [1]

[1] The problem of a high false positive rate has been identified mother contexts. In a 1983 study of the use of polygraph testing, OTA concluded that "the mathematical chance of incorrect identification of innocent persons as deceptive (false positives) is highest when the polygraph is used for screening purposes " This is because in screening situations, there is only a very small percentage of the group being screened that might be guilty U S Congress, Off Ice of Technology Assessment, *Scientific Validityof Polygraph Testing: A Research Review and Evacuation,* OTA-TM-H-15, Washington, DC Government Printing Office, November 1983, p 5

SOURCE: Off Ice of Technology Assessment, 1995.

Analysts at FinCEN and law enforcement agencies have little expertise analyzing wire transfers on the scale envisioned by proposals, and until they do, it will be difficult or impossible to construct a traditional knowledge-based system to analyze wire transfers automatically.[32] Another problem stems from the paucity of information contained in a wire transfer. At best, the wire transfer message contains only the names, address, and account numbers of the originator and beneficiary, information about intermediary banks processing the transfer, the amount of the transfer, and optional payment instructions. At worst, the message identifies the banks involved in the particular transfer and the account number of the beneficiary. Such information, unless combined with large amounts of other data, offers few opportunities to identify suspicious transfers.

Even wire transfer systems know surprisingly little about the transfers that flow over their systems. For example, the Federal Reserve Banks only collect information on the total dollar volume and number of transfers processed over Fedwire. The sole exception appears to be a 1987 study of a single day's traffic on CHIPS and Fed-

[32] FinCEN has attempted to arrange a pilot study to examine Fedwire data. However, there is no indication that the legal issues surrounding access to wire transfer data have been overcome.

wire.[33] However, even this study has severe limitations. It sampled only certain categories of the day's traffic and examined only wire transfers from some participating banks.

### Patterns in Time and Space

If reliable indicators of money laundering activities are present in financial data, they may necessarily involve multiple transfers over a period of time between geographically dispersed individuals, businesses, and financial institutions. For example, known scenarios of money laundering involve a series of cash deposits into multiple accounts (where each deposit is under the $10,000 reporting threshold), aggregation of the funds into a separate account, and a large wire transfer out of that separate account.[34] Being able to screen for such patterns necessarily involves temporal and spatial concepts.

The need for temporal and spatial screening affects the necessary technical characteristics of a successful monitoring system. First, it emphasizes the importance of examining data from multiple locations and time periods, making localized analysis less likely to be effective—screening at a single bank or for limited time periods may identify relatively few money laundering schemes. Second, the need for temporal and spatial screening implies the need for certain types of databases and analysis tools, making them ill-suited for investigating money laundering. Some tools, particularly those developed for law enforcement (e.g., NETMAP), do allow analysis using temporal and spatial information.

### Dynamic and Diverse Forms of Criminal Conduct

There are many ways to launder money. Any system that attempts to identify money laundering will need to evaluate wire transfers against multiple profiles. In addition, money launderers are believed to change their modes of operation frequently. If one method is discovered and used to arrest and convict money launderers, activity will switch to alternative methods.[35]

Law enforcement and intelligence community experts interviewed by OTA stressed that criminal organizations engaged in money laundering are highly adaptable and flexible. For example, in the past two years, law enforcement agencies have seen increased use of nonbank financial institutions (e.g., exchange houses and check cashing services) and increased use of instruments like postal money orders, cashiers checks, and certificates of deposit.[36] In this way, money launderers resemble individuals who engage in ordinary fraud. They are adaptive and devise complex strategies to avoid detection. They often assume their transactions are being monitored and design their schemes so that each transaction fits a profile of legitimate activity.[37]

### Similarity of Licit and Illicit Conduct

Many patterns of transactions associated with money laundering differ little from legitimate transactions (see chapter 1). They are recognizable only because of their association with criminal activities. Banking officials emphasize that legitimate wire transfer activities in the U.S. bank-

---

[33] Federal Reserve Bank of New York, *A Study of Large-Dollar Payment Flows Through CHIPS and Fedwire*, December 1987.

[34] This scenario is also consistent with legitimate activity of some small businesses.

[35] One convicted money launderer insists that criminal organizations will know "instantly" when money laundering detection methods are changed, because they have friends in banking, law enforcement, and intelligence communities. Kenneth Rijock, interview at OTA October 6, 1994.

[36] "Current Trends in Money Laundering," Hearing before the Permanent Subcommittee on Investigations, Committee on Government Affairs, U.S. Senate, 102 Congress, Second Session, February 27, 1992.

[37] Malcolm Sparrow, "The State of the Fraud Control Game; and the Impact of Electronic Claims Processing on Fraud and Fraud Control," Unpublished paper for the 1994 International Symposium on Criminal Justice Information Systems and Technology, 1994.

ing system are diverse and wide-ranging, differing in their type, purpose, frequency, origins, destinations, and amounts. Because the ordinary traffic is so heterogeneous, it can be difficult to identify transfers that are "out of the ordinary."

Wire transfer information alone is not enough to determine legality.[38] Money laundering experts told OTA that it is nearly impossible to identify individual wire transfers as suspicious.[39] Most illegitimate uses of wire transfers mirror standard business practices. Officials at the Federal Reserve maintain that all patterns with which they are familiar are also consistent with normal business practices.

Instead, only patterns of transactions (both wire and nonwire) can indicate money laundering. Indeed, even these patterns of transactions can be made to resemble legitimate businesses. However, these data can be combined with other data in order to evaluate the suspiciousness of a pattern of financial transactions. This is one reason why every major effort to search for money laundering in financial data (e.g., those of FinCEN and AUSTRAC) employs link analysis. When data from law enforcement databases are included with financial data, it becomes more feasible to separate licit and illicit activities.

### *Multiple Levels of Analysis*

It is useful to think of wire transfer analysis as consisting of multiple levels.[40] First is the transaction level. Money laundering necessarily involves a set of individual transactions such as currency deposits and withdrawals, wire transfers, and checks.[41] Second is the individual or account level. Multiple transactions are associated with specific individuals and bank accounts.[42] Third is the business or organizational level. An individual business may be a front for money laundering and may involve multiple accounts and multiple individuals. Fourth is the "ring" level which involves multiple businesses, accounts, and individuals in a money laundering scheme of broad scope.

The multiple levels of possible analysis indicate a flaw in analytic approaches that only examine transaction-level data. Schemes that operate at a "ring" or a business level may not be detectable through transaction analysis. Instead, the indicia of these schemes may become apparent only after aggregating data to the individual/account, business, or ring level. Analysis at any single level may miss indicators of activity at other levels. Different levels of analysis may be best done in different places. For example, banks are uniquely equipped to detect money laundering at the transaction and individual/account levels. They have access to customer information and account history which can be brought to bear on evaluating suspiciousness. In contrast, FinCEN is uniquely equipped to detect money laundering at the business and ring level. They have aggregated data and additional information from law enforcement and commercial sources that can be brought to bear.

---

[38] Mike Harrington and Marcus Glenn, "Methods for Analyzing Wire Transfer Data To Detect Financial Crimes," MTR-91-W00057, McLean, VA: MITRE Corporation.

[39] Many people compare the problem of looking for illicit wire transfers to "looking for a needle in a haystack." Ted Senator, Chief of FinCEN's Systems Development Division, notes that the problem is more analogous to "looking for a needle in a stack of other needles." Even if you examine each transfer, it is not obvious which ones are illicit.

[40] This idea is adapted from: Malcolm Sparrow, "The State of the Fraud Control Game; and the Impact of Electronic Claims Processing on Fraud and Fraud Control," Unpublished paper for the 1994 International Symposium on Criminal Justice Information Systems and Technology, 1994.

[41] However, some forms of money laundering involving bulk shipments of currency out of the United States would not involve any transactions that could be captured by monitoring U.S. institutions.

[42] FinCEN's AI System (FAIS) consolidates transactions into precisely these categories: subjects and accounts.

## FINDINGS

- Many of the major challenges in constructing an effective wire transfer analysis system are related to data and not technology. In several cases, technologies are available that would be appropriate for wire transfer analysis, but data and expertise do not exist to make those technologies effective.
- There are two basic types of screening technologies: knowledge-based systems and link analysis. Effective use of knowledge-based systems requires either human experts who can accurately screen wire transfers or substantial amounts of data for which the correct analysis is already known. Effective use of link analysis requires a variety of readily available data, some of which provide indicators of money laundering activity.
- In general, there are no experts or data to make the use of knowledge-based systems feasible for detecting money laundering through wire transfer monitoring alone. However, data are available that would make it possible to conduct link analyses on wire transfers.
- The data and expertise necessary to apply link analysis already are assembled at FinCEN (the Financial Crimes Enforcement Network).

# 5 Privacy and Confidentiality[1]

The wire transfer monitoring systems proposed in chapter 7 share the feature of increasing government access to wire transfer records. Wire transfers are the medium of choice for large corporate payments requiring immediacy, security and certainty, and wire transfers are a vital part of the operation of the modern industrial and service economies of the United States and the world. Corporations use wire transfer systems to move capital, buy stocks and pay for international and domestic trade. Private parties also use the wire transfer medium to move money expeditiously, and some experts forecast that individuals will increasingly come to utilize wire transfers as an integral part of home banking, although the advent of digital money may prove a more facile means of moving money in the future (see box 7-4 in chapter 7).



[1] This chapter and the next will use the term "confidentiality" to refer to relationships wherein parties, contractually or otherwise, keep information secret. "Security" refers to safeguards undertaken to prevent unauthorized access to information. "Privacy" refers to policy debates regarding the balance struck between the interests of individuals in liberty and the interests of society in a stable social order. This balance is struck in court cases and legislation and is always subject to modification. Consider the recent bombing in Oklahoma City. According to the *Washington Post*, the government wishes to create a counterterrorism center, with a new mission of "intercepting digital communications." *Washington Post*, June 11, 1995, p. F7. This, and the antiterrorism bill nearing enactment, will likely reduce individuals' privacy in electronic communications.

One significant difference between enhanced counterterrorism measures and the monitoring of wire transfer systems would be that in the former case, arguably all citizens will have a reduced expectation of privacy and all citizens will benefit (i.e., from a reduced threat of terrorism). In the case of wire transfers, however, a small set of parties will have their confidentiality compromised and receive little, if any, direct benefit in return. Society as a whole benefits from reduction in the amount of money laundering, while the costs of that reduction are borne by a limited set of actors.

Each of the configurations discussed in chapter 7 would increase the government's access to domestic wire transfer records, with little or no requirement of individualized suspicion. Some configurations would require government collection and retention of an unprecedented volume of data; the government would come to possess a great chunk of the financial aspect of the stream of commerce. This access first represents an archetypal communications privacy issue, harking back to court cases such as *Berger* v. *New York* and *Katz* v. *United States* and the legislative debates surrounding wiretapping, from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to the recent Communications Assistance for Law Enforcement Act of 1994.[2] Second, government access to wire transfer records would represent a substantial diminution in financial privacy. Third, the subsequent manipulation of the wire transfer data, relating them to other financial or personal data, is computer matching—a practice termed by one noted commentator as "one of the most vexing privacy issues of the 1980s" and "one of the most virulent forms of surveillance practiced by any government."[3] In either case, some of the proposed technological configurations conjure up the image of the computer state, where all data, no matter how innocuous or elliptical in itself, may be collected, aggregated, manipulated, and cross-correlated with other databases to the point where it becomes information with a context and no longer innocuous.[4]

Privacy commentators bring different viewpoints to the privacy and confidentiality issues raised by the wire transfer monitoring proposals. Some privacy advocates view this question primarily as governed by Constitutional standards and policy, articulated by the Fourth Amendment and 200 years of jurisprudence and legislative enactments, finetuning the balance between the interests of law enforcement and the individual. Other commentators, influenced by "fair information practices," view this problem as primarily one of impermissible "secondary use," or the injunction against the use of information beyond the purpose for which it was collected (see box 5-1).[5] Both groups of privacy advocates would be

---

[2] *Berger,* 389 U.S. 41 (1967), *Katz,* 389 U.S. 347 (1967)(*Berger* and *Katz* were the Supreme Court's watershed decisions to extend Fourth Amendment protections to telephonic communications); Title III, Pub. L. 90-351 (June 19, 1968)(the legislative response to *Katz* and *Berger*); the Communications Assistance for Law Enforcement Act of 1994, Pub. L. 103-414 (Oct. 25, 1994), requiring the telecommunications industry to assist law enforcement agencies in matching intercept needs with modern communication technology. See the OTA report *Electronic Surveillance in a Digital Age*, analyzing the costs associated with facilitating law enforcement wiretapping of digital switches. U.S. Congress, Office of Technology Assessment, OTA-BP-ITC-149 (Washington, DC: U.S. Government Printing Office, July 1995).

[3] David H. Flaherty, *Protecting Privacy in Surveillance Societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: The University of North Carolina Press, 1989), p. 344. "The current enthusiasm for matching programs is a typical search for a simple panacea for large problem that in some ways are almost hopeless; the enthusiasm is even greater, at least for a time, because the 'fix' is technological." *Ibid.* at 345. Flaherty focuses on the loss of individual liberty through governmental computer matching/data linkages intended to root out fraud and abuse of government benefits programs. Another author underscores the threat to privacy posed by computer matching. John Shattuck, "In the Shadow of *1984*: National Identification Systems, Computer-Matching, and Privacy in the United States," 35 *Hastings Law J.* 991-1005, pp. 991-2 (July 1984)(noting also the Internal Revenue Services's (IRS) planned use of commercial data bases to generate lifestyle profiles to catch tax cheats). It should be noted that the Computer Matching Act and Privacy Protection Act of 1988 does not apply to law enforcement/national security matching of records.

[4] One noted information privacy expert, Professor Joel Reidenberg of Fordham Law School, goes further and terms any wire transfer monitoring proposal a "quantum leap towards the surveillance state."

[5] In 1973, the former Department of Health, Education, and Welfare articulated one of the earliest versions of the principles underlying fair information practices. The third principle stated that "there must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent," a classic formulation of the injunction against secondary use. U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (Washington, DC: 1973), p. 41, *cited in* The Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington, DC: 1977), p. 15, fn. 7.

## BOX 5-1: Fair Information Practices and the Fourth Amendment

Fair information practices limit the secondary use of data, independent of the nature of the data subject and independent of the party conducting the secondary use. The Europeans have taken the lead in the application of fair information practices, although in the early 1970s, the United States promulgated the former Department of Health, Education and Welfare and Office of Management and Budget fair information practices guidelines governing information practices in the federal government. Reidenberg and Gamet-Pol applaud European data protection laws for their comprehensive treatment of the balance between information privacy and the freedom of informational These authors suggest that the United States' piecemeal and sometimes inadequate guarantee of information privacy is coming under the active interest of the Europeans, and that the U.S. will have to start responding to this foreign trend in order to avoid lost business opportunities by the U.S. information industry.[2]

Corporations in the United States have incorporated fair information practices into their charters and bylaws to regulate their treatment of information. Questions remain whether fair information standards should extend to cover individuals *and* corporations, or even whether corporations themselves desire the protections. While individuals may share with corporations the fear that information about them may be manipulated to their economic detriment, individuals and corporations share few other concerns, such as the individual's desire for physical safety, avoidance of embarrassment or hurt feelings (protected by the tort of public disclosure) and for freedom to communicate political thinking without fear

The further question arises whether the prohibition against secondary use should govern law enforcement conduct, Advocates in favor of extending the scope of fair information practices to criminal matters have the burden of squaring fair information practices with this country's long tradition of applying the Fourth Amendment to decide the question of what information may be properly gathered and used against criminal defendants. Thus far, this case has not been made, apart from the argument that European data protection standards may prove an impediment to U.S. corporations seeking to transfer and process data across international borders. While the European Union (EU) has made a point of treating public and private data protection equivalently, the pending EU Data Protection Directive contains two provisions contemplating special treatment of law enforcement and its need to process data to conduct its mission. (See chapter 6 for more detail on the international aspects of data protection.)

[1] Joel Reidenberg and Francoise Gamet-Pol, "The Fundamental Role of Privacy and Confidence in the Network, " 30*Wake Forest L. Rev 105-125* (Spring 1995), p 117

[2] Ibid,, p. 119.

SOURCE Office of Technology Assessment, 1995.

alarmed by the loss of control over personal information and fears of inaccuracy and obsolescence in collected data.[6]

Ordinarily, recourse to analogy helps guide analysis of new problems in policy and law. But in this case, while many analogies may be suggested,

[6] It should be noted at the outset that individuals no longer own, possess or even enjoy dominion over their personal data. See, e.g., Shattuck "Computer-Matching," op. cit., footnote 3, p. 995. Doctrines of "information privacy" and "data protection" are an attempt to restore some control to the individual over data identifying the individual. See, Office of Management and Budget, National Information Infrastructure *Draft Principles for Providing and Using Personal Information, 60 Fed.Reg. 4362, 4363* (January 20, 1995) (''information privacy" defined as "an individual claim to control the terms under which personal information-information identifiable to an individual—is obtained, disclosed and used").

none are completely apposite. Already, two analogies have been suggested—wiretapping and computer matching. Neither fully captures the nature of wholesale wire transfers and all the issues inherent in some of the technological configurations. Other possible analogies for a "screening" system include: a) sobriety checkpoint roadblocks, as litigated in *Sitz* v. *Michigan State Department of Police*;[7] b) the airport courier drug profile;[8] and c) the questioning of passengers on a stopped long-haul bus, *Florida* v. *Bostick*.[9] While these analogies raise the idea of the "profile," a set of characteristics putatively separating the innocent from the suspicious, they all fail in one respect. They do not capture the fact that most of the technology configurations would retain funds transfer data, perhaps even wire transfers not immediately associated with some profile as "suspicious."

That the dominant users of the various wire transfer systems are currently corporate further complicates the analysis. Compared to the individual right of privacy, the corporation enjoys only a reduced right of confidentiality—a right premised on a concern for economic detriment through the loss of confidential business information. Recent court cases and legislation have confirmed the merits of conferring on corporations some measure of protection, however.[10] For many commentators, particularly those who anchor the right to privacy on its role in preserving the free exchange of political ideas, the corporation's privacy interests in this matter may amount only to a feather's weight, as set against "the stone" of the law enforcement interest in stemming the flow of illicit money.[11] There are others, however, who fashion a principled basis for finding a corporate interest in confidentiality, particularly Judge Richard Posner, who places a higher premium on corporate privacy than individual privacy.[12]

---

[7] 496 U.S. 444 (1990)(holding constitutional a police roadside blockade where all motorists along a highway were briefly detained and screened for signs of intoxication; some 1.5 percent were arrested out of those detained). *Sitz* is partially distinguished by the public nature of traveling on a highway; by contrast, current law provides a measure of confidentiality to domestic wire transfers in electronic transit and storage.

[8] Federal and local law enforcement agents have developed crude profiles setting forth characteristics of drug couriers traveling via airplanes, buses and trains. Agents scrutinize disembarking passengers against the backdrop of the profile, approaching those suspected of carrying narcotics and asking if they might search their baggage. See, e.g., *United States* v. *Sokolow*, 490 U.S. 1 (1989)(the agent's use of a "drug courier profile" to identify the defendant did not taint the detention and later arrest, even though the profile might be consistent with innocent behavior). A glaring dissimilarity here would be the agents' right to be in the public spaces of bus and train terminals and airports, in contrast to the currently confidential nature of wire transfer systems (consider that Fedwire requires subpoenas of even Federal Reserve employees before they may examine wire transfer records).

[9] 501 U.S. 429 (1991)(upholding the constitutionality of searches and seizures where agents boarded long-haul buses during scheduled stops and applied courier profiles to the passengers). Another analogy suggested is the Bank Security Act (BSA) data itself, e.g., the Ccurrency Transaction Report (CTR) and Currency or Monetary Instruments Report (CMIR), although these forms are distinguished by the fact that they are specifically created for the government, and not used outside of their intended purpose, namely the detection of money laundering and other forms of financial crime. Hence, they are not put to a troubling secondary use beyond their intended purpose.

[10] See *Tavoulareas* v. *The Washington Post Company*, 724 F.2d 1010, (D.C. Cir.); *vacated* and *remanded*, March 15, 1984; see also the Electronic Communications Privacy Act of 1986 (applying to individuals and corporations alike).

[11] Telephone interview with Professor Alan F. Westin, August 25, 1994. Westin recognizes the corporation's right to engage in the decision-making process in private, and, also, the right to associate with others privately.

[12] Richard Posner, *The Economic Analysis of the Law* (Cambridge, MA: Harvard University Press, 1981), p. 248. "Secrecy is an important method for the entrepreneur to appropriate the social benefits he creates, but in private life secrecy is more likely to operate simply to conceal discreditable facts." See also, George Trubow, "Whether and Whither Corporate Privacy," to be published in *DataLaw Report* and Anita L. Allen, "Rethinking the Rule Against Corporate Privacy Rights: Some Conceptual Quandaries for the Common Law," 20 *John Marshall L. Rev.* 607-639 (Summer 1987).

Some privacy advocates resist linking the terms "corporation" and "privacy,"[13] in part because the corporation lacks the psychological apparatus to take offense at intrusions into protected zones and perhaps, because historically privacy advocates have viewed direct marketing companies and other corporations as violating the privacy of individuals. Other privacy advocates influenced by fair information practices condemn all secondary uses of information, independent of whether the data is generated by a corporation or individual and regardless of whether government or corporations are scrutinizing data for the secondary purpose.[14] Some European nations, including Austria, Luxembourg and Norway, extend data protection principles to corporate entities. Yet fair information practices have not uniformly been adopted or practiced by U.S. corporations to protect consumers, so it would appear to be honoring the principle too much to extend their benefits to the corporation. Significantly, the Business Roundtable expressly demurred at protecting legal persons, or corporations, principally out of a fear that competitors could demand access to files held on them by other corporations, a central tenet of fair information practices.[15]

## CONSTITUTIONAL AND LEGISLATIVE PERSPECTIVES ON FINANCIAL PRIVACY

### Privacy Jurisprudence

*United States* v. *Miller*, 425 U.S. 435 (1976), remains the state of constitutional jurisprudence on the question whether individuals enjoy under the Fourth Amendment a "reasonable expectation of privacy" in financial records created or maintained by a bank in the course of ordinary business dealings.[16] In 1976, the Supreme Court answered the question in the negative. Some commentators have criticized the ruling as well as the incomplete attempt of Congress through the Right to Financial Privacy Act of 1978 (RFPA) to undo the effects of *Miller.* But the Supreme Court is unlikely to revisit the issue in the near future, because RFPA approximates the procedural protections of the Fourth Amendment for financial privacy and also because the *Miller* case rests on old and broad precedent undermining the ability of individuals to contest government access to records held by

[13] "Virtually everybody agrees that privacy, by definition, is uniquely a personal right. Artificial persons, as opposed to natural persons, do not enjoy a right to privacy." Robert Ellis Smith, *The Law of Privacy in a Nutshell* (Providence, RI: Privacy Journal, 1993), p. 48.

[14] The Code of Fair Information Practices, currently being updated by the Information Infrastructure Taskforce for the National Information Infrastructure under the aegis of the Office of Management and Budget (OMB), would also militate against secondary use of wire transfer data. *Draft Principles for Providing and Using Personal Information through the Office of Management and Budget*, 60 Fed. Reg. 4362 (Jan. 20, 1995).

[15] Business Roundtable Statement on Transborder Data Flow, *reprinted in* L. Richard Fischer, *The Law of Financial Privacy: A Compliance Guide* (2nd ed.)( Boston: Warren, Gorham & Lamont, 1991), 6-89, A6.3.

[16] The Fourth Amendment provides that the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

third parties, such as banks or accountants.[17] Some states have found state constitutional protection for financial records, however: in California, the state Supreme Court held that a customer "has a reasonable expectation that the bank would maintain the confidentiality of checks originated by the customer and of bank statements generated by the bank."[18] Today, the federal and California state protections for financial information are roughly equivalent, although they originated from opposing constitutional starting points.[19]

Nevertheless, it is useful to scrutinize the roots of the Fourth Amendment and its interpretations to weigh the intrusion of government access to payment systems information. Specifically, some argue that in the Fourth Amendment and the Bill of Rights generally the Founding Fathers sought to guard against the excesses of law enforcement tactics used by European nations, particularly the general warrant and writs of assistance: John Adams wrote that, when James Otis argued against general writs in 1761, "the child Independance [sic] was born."[20] (See box 6-1 in chapter 6 for discussion of a modern case with general subpoena implications.)

Alan Westin, in his seminal *Privacy and Freedom*, catalogs the values protected by the Bill of Rights, from the First Amendment and Justice Story's solicitude for "private judgment" and "private sentiment" to the concern for the home as a

---

[17] The *Miller* Court held that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party, or bank] to government authorities. . . ." 425 U.S. at 443. *Miller* follows *First National Bank* v. *United States*, 267 U.S. 576 (1925) and *Donaldson* v. *United States*, 400 U.S. at 522 (both cases holding that a summons served upon third parties violates the Fourth Amendment rights of neither the target nor the third party); see also *California Bankers Ass'n* v. *Shultz*, 416 U.S. 21 (1974), insofar as *Shultz* reaches the merits of privacy issues. In addition, the Supreme Court underscored the vitality of *Miller* in 1984, when it ruled that an individual had no reasonable expectation of privacy in confidential financial records given to and maintained by broker/dealer firms. *S.E.C.* v. *Jerry T. O'Brien, Inc*., 467 U.S. 735 (1984). At the core of these decisions lies the judicial finding that the individual does not own or possess the records that are held by a third party business. *Miller*, 425 U.S. at 440 (the customer "can assert neither ownership nor possession" of the records—in fact they are business records of the bank). Within two years, Congress responded to *Miller* with the RFPA. In contrast, when the Supreme Court found no constitutional right to be free from wiretapping in *Olmstead*, there was no express congressional response. Law enforcement wiretappings continued for forty years largely unfettered until the *Katz* decision and Title III circumscribed the practice of the telephonic wiretap, mandating a court order and special procedures to minimize the intrusion to legitimate telephonic conversations.

[18] *Burrows* v. *Superior Court*, 520 P. 2d 590 (Ca. Sup. Ct. 1974). *See also* Fischer, *The Law of Financial Privacy, op. cit.*, footnote 15, ¶5.04[4][a] (writing that Colorado, Florida, Illinois and Pennsylvania have followed the California rule, finding that state constitutions required legal process before access is permitted to bank-held financial information). Utah, California and Pennsylvania also confer some privacy rights to the corporation. It should be emphasized that although Congress may legislate based on the Commerce Clause and Supremacy Clause to pre-empt state constitutional protections, direct reversals by Congress of state constitutions are relatively rare. Article VI, clause 2 of the U.S. Constitution provides:

> This Constitution, and the laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the authority of the United States shall be the supreme law of the land; and the judges in every state shall be bound thereby, any thing in the constitution or laws of any state to the contrary notwithstanding.

[19] Richard Fischer, OTA Workshop, Feb. 16, 1995. It should be noted at this juncture that the Fifth Amendment does not protect bank records either. The Fifth Amendment requires that documentary evidence be generated by the one claiming the Fifth Amendment right—not apposite in the financial records context. See, e.g., *Fisher* v. *United States*, 425 U.S. 391 (1976)(an individual cannot assert the Fifth Amendment to shield accountant-generated records from government subpoena).

[20] The Founding Fathers decried the general warrant and writ of assistance in the strongest of language, for "their indiscriminate quality, their license to search Everyman without particularized cause" (John Adams) and they were considered to be "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book," (John Otis), quoted by Nadine Strossen, "Individual Rights After *Sitz*," 42 *Hastings L.Rev.* 285, 353-54 (Jan. 1991). Strossen is particularly alarmed by this form of search, which is aimed not at gathering evidence on known wrongdoers, but rather at turning up previously unidentified and unsuspected offenders, *ibid.*, p. 355. The Founding Fathers were greatly concerned with the suspicionless entries into homes and businesses sanctioned by the general warrant and writs of assistance. In this view, the Framers intended that the Fourth Amendment prevent police from interfering with personal freedom unless the police had already formed particularized suspicion as to wrongdoing.

castle embodied in the antiquartering provision of the Third Amendment and the Fourth Amendment's express protection of papers and the home.[21] One may reasonably infer that the Bill of Rights places a premium on the sanctity of the mind and home, codifying a "rhetoric of domesticity" and the intellect, particularly political thoughts and speech.[22] Passages from Justice Brandeis's dissent in *Olmstead* v. *United States* confirm this view:

> The makers of our Constitution. . .recognized the significance of man's spiritual nature, of his feeling and of his intellect . . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. 277 U.S. 438, 478 (1928).

And in a widely quoted prescient piece of his dissent, Brandeis notes:

> . . . the progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thought and emotions. *Ibid*., at 474.

More recently, in assessing the constitutionality of the Bank Secrecy Act (BSA) in the case of *California Bankers Ass'n* v. *Shultz,* the Court distinguished *Shultz* from *Stanford* v. *Texas*, where the Court had ruled that a warrant permitting the search and seizure of defendant's "books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments concerning the Communist Party of Texas" was an unconstitutional general warrant.[23] Instrumental to the reasoning in *Shultz* was that the BSA data did not involve "rummaging around records of the plaintiffs, nor do the reports . . .deal with literary material as in *Stanford*; the information sought is about commerce, not literature."[24]

Thus, for nearly two centuries, the Supreme Court confined the scope of the Fourth Amendment to its plain text, to "persons, houses, papers, and effects." And in 1968, the Court extended the protections of the Fourth Amendment to "people not places," in protecting telephonic communication from a public phone booth.[25] But should the policies behind the Fourth Amendment further extend to and protect corporations and their financial communications in the stream of commerce?[26]

---

[21] Alan F. Westin, *Privacy and Freedom* (New York: Athenaeum, 1967), pp. 330-333. Westin's express linkage between privacy and freedom in the title intimates his emphasis upon the utility of privacy in maintaining a free and democratic society. This linkage is harder to perceive when the information is in the stream of commerce, of course.

[22] David J. Seipp, *The Right to Privacy in American History* (Cambridge, MA: Harvard University, 1978).

[23] 416 U.S. 21, 62 (1974).

[24] The specific Bank Secrecy Act (BSA) report discussed in *Shultz*, Foreign Bank Account Reports (FBARs), represent a mere fraction of the amount of international commerce that would be reported under any proposed monitoring system, weakening the precedential import of *Shultz*.

[25] This quoted phrase stems from *Katz* v. *United States*.

[26] Pre-electronic analogs for wire transfer payments would be checks, and for most of this nation's history, checks received no special protection from the scrutiny of law enforcement. At the same time, as is evident in the text, the telecommunications aspect of the wire transfer complicates the analysis, adding a concern for interception of electronic communications.

The Supreme Court's recent pronouncement on the Commerce Clause in *United States* v. *Lopez*, (No. 93-1260)(April 26, 1995) does not threaten Congressional power to regulate wire transfers. The *Lopez* Court held that the Gun-Free School Zones Act of 1990, which criminalized the possession of guns in a "school zone," exceeded Congressional authority to regulate commerce under the Commerce Clause of the federal Constitution and reaffirmed the federalism at the core of this Republic. Nevertheless, this ruling would not threaten the power of Congress to regulate wire transfers, which are close to the heart of interstate, and indeed, international commerce.

**BOX 5-2: Major Supreme Court Cases on Privacy and Financial Privacy**

- *Olmstead v. United States* (1928): The Supreme Court of the United States holds that the Fourth Amendment does not protect telephonic communications, even when the wiretap is achieved by physical trespass at the target's home.
- *Katz v. United States (1 967):* Reversing *Olmstead,* the Supreme Court holds that the Fourth Amendment protects "people, not places, " in finding that the bugging of a public telephone booth habitually used by the target of an investigation requires a warrant based on probable cause.
- *California Bankers Association v. Shultz* (1974): The Supreme Court upholds the constitutionality of the Bank Secrecy Act's reporting requirements, upholding the constitutionality of the Bank Secrecy Act against challenges based on the First Amendment right to privacy and anonymity in associations, the Fourth Amendment reasonable expectation of privacy and the deprivation of due process by imposition of unreasonable compliance costs on banks. It should be noted that the Court did not reach some of the most interesting arguments for purposes of wire transfer monitoring, to wit, whether depositors in excess of $10,000 had a Fourth Amendment violation to allege.
- *United States v. Miller (1976):* The leading case on financial privacy, in which the Supreme Court found no reasonable expectation of privacy and hence no Fourth Amendment protection for financial records held by third parties, such as financial institutions. This result is largely undone by the subsequent Congress, which enacted the Right to Financial Privacy Act, establishing a presumption of privacy in bank-held records.

SOURCE. Office of Technology Assessment, 1995.

In *Dow Chemical,* the Supreme Court obliquely suggested another constitutional issue.[27] The Supreme Court ruled that the government did not violate Dow Chemical Corporation's rights under the Fourth Amendment by flying over a manufacturing plant in a chartered plane and photographing the plant with commercial photographic equipment. The Court went on to suggest that if the government had not relied upon a commercial aviation photographer (by using alternatively a spy satellite, for example), perhaps the Court would have found that the corporation had a reasonable expectation of privacy. This suggests that the fact that the government observes a defendant from a legitimate vantage point (either from public airspace or from within the stream of commerce) does not insulate the government from charges of unconstitutional conduct: it is necessary to inquire as to the means of scrutiny. In the context of wire transfers and massive data matching by large computers, this line of analysis is partially undercut by the growing reliance of direct marketers on massively parallel computing for ever more sophisticated targeting of customers for their clientele. No longer is supercomputing the exclusive province of the federal government (see box 5-2).

## The Statutory Picture

Any congressional decision on government access to wire transfer data will not be made *de novo.* Any of the technological configurations proposed in chapter 7 would represent a rollback of current privacy protections under law and would also represent a step back from the first recommendation of the U.S. Privacy Protection Study Commission, which recommended that Congress provide an expectation of confidentiality in records held by financial institutions, requiring that govem-

[27] *Dow Chemical Co.* v. United States, 476 U.S. 226, 238-239 (1986). The relevant language from Dow Chemical is what lawyers refer to as *dicta. Dicta* is speculative reasoning not logically essential to the ruling in a case, and hence not binding upon future cases.

ment show clear proof of the relationship of any record sought and a violation of law.[28]

Federal and state legislation and judicial pronouncements on privacy have made data protection a "patchwork quilt."[29] In addition, section 1515 of the Annunzio-Wylie Anti-Money Laundering Act of 1992 mandated that the Secretary of the Treasury promulgate international wire transfer recordkeeping provisions and authorized the Secretary to "request" copies of international wire transfer records from banks.[30] This provision has not been tested yet, as the recently issued wire transfer recordkeeping regulation does not take effect until January 1, 1996. In addition, the U.S. Treasury Department has interpreted its authority under the BSA, specifically 31 U.S.C. 5314, as authorizing Treasury to issue regulations requiring specified banks to disclose "wire fund transfers" with foreign financial agencies.[31]

Neither section 1515 of Annunzio-Wylie nor the "targeting" regulation addresses government access to domestic wire transfer records. Neither has the judiciary squarely addressed this issue. Some experts believe that the Electronic Communications Privacy Act (ECPA)[32] should control the analysis and prohibits access to the information,[33] while others maintain that ECPA does not cover wire transfers at some points in their life cycle through various banks.[34] The Federal Reserve Board's Office of General Counsel and others believe that RFPA should be viewed as the paramount statute, although some federal courts have held that the Act does not protect all wire transfer information. At least one court has so ruled because the wire travels through banks and wire transfer instrumentalities in which neither the originator nor the recipient holds an account.[35]

The protections afforded by RFPA and ECPA differ in material respects, a byproduct of the United States' piecemeal approach to privacy protection. While RFPA, by its letter and judicial interpretation, does not accord its limited protections to corporations and partnerships of greater than five partners,[36] ECPA applies to all "users" of an "electronic communications service." The statutes also differ in terms of the degree of protection afforded information, as well as the procedural requirements that must be adhered to before the release of information to law enforcement. For instance, under some circumstances RFPA requires that notice be provided to the bank custom-

---

[28] The Privacy Protection Study Commission, *Personal Privacy in an Information Society, op. cit.*, footnote 5, pp. 362-363.

[29] Wayne Madsen, *Handbook of Personal Data Protection* (New York: Macmillan Publishers Ltd, 1992), p. 108.

[30] The Annunzio-Wylie Anti-Money Laundering Act of 1992 (Pub.L No. 102-550, Title XV), with section 1515 codified at 12 U.S.C. 1829b(b)(3).

[31] 31 C.F.R. 103.25(a) and (b)(2).

[32] Pub. L. 99-508. In short, ECPA created a reduced right of privacy in electronic communications, supplementing Title III's more robust protection of telephonic communications.

[33] This group includes the OCC and the Office of Legal Counsel, Department of Justice, which opined that ECPA, not RFPA, controls electronic access to Fedwire data, relying in part upon lower courts' holdings that RFPA does not address intermediary banks' actions with respect to wire transfers for non-customers. OLC Opinion by Dellinger, September 13, 1993. The opinion rules that no judicial process is necessary to access records once they have been transferred to microfiche.

[34] Some support for this latter position may be found in the recent Fifth Circuit case, *Steve Jackson Games*, to the extent that the court's non-intercept analysis for e-mail may be extended to the transmission of wire transfers. *Steve Jackson Games v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994); *Steve Jackson Games* v. *United States Secret Service*, 816 F.Supp. 432 (W.D.Texas 1993) (finding no interception of unread e-mail stored on an electronic bulletin board since the acquisition of the e-mail was not contemporaneous with its transmission).

[35] *United States* v. *Daccarret*, 6 F.3d 37, 51-52 (2nd Cir. 1993)(holding RFPA as not protecting defendant Daccarret *et al.*, in part because they did not maintain an account in their names at the intermediary banks from which the wire transfers were seized).

[36] The Privacy Act also extends its limited protections solely to individuals.

er before the record is released, giving the customer an opportunity to invoke judicial process to quash the disclosure to law enforcement.[37]

While the first title of ECPA protects against the interception of electronic communications, the Stored Wire Act, Title II of ECPA, concerns itself with communications in "electronic storage" and sets out restrictions on the conduct of "electronic communications service providers:"[38]

> Any person or entity providing an electronic communications service to the public may not knowingly divulge to any person or entity the contents of an electronic communication while that communication is in electronic storage. 18 U.S.C. 2702(a)(1), see also S. Rep. No. 99-541, at 37.

"Electronic storage" is a term of art, signifying:

> A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. 2510(17).

Reporting of wire transfer information, either while in temporary storage while in transit or afterwards while stored for backup protection would thus violate ECPA.[39] Neither ECPA nor its legislative history give a sense to how long "backup protection" may go on, so it could be argued that long-term electronic storage of wire transfer messages would not merit protection. Nonetheless, ECPA specifically protects messages stored for more than 180 days and the wire transfers most interesting to law enforcement are apt to be relatively fresh, in any case.

The statute permits disclosure to law enforcement upon issuance of a court order, warrant or administrative subpoena, depending on the duration of the electronic storage.[40] (See box 5-3). If the electronic service provider, in this case a bank, inadvertently reads the electronic communication and discovers criminal conduct, release of the communication to law enforcement is permitted, giving rise to the negative implication that moni-

---

[37] Several privacy principles may be derived from the statutes: for one, the uses and limits of Title III, the Wiretap Act, as a model for serious forms of government intrusion, necessitating judicial, or at a minimum, grand jury sanction; as well as the curative effect of notice, in terms of impeding secret government files and actions. Notice to the customer may be waived under RFPA in cases where there is reason to believe that notice will result in: endangered life; flight from prosecution; destruction of evidence; intimidation of potential witnesses or serious jeopardy to the investigation or proceedings. 12 U.S.C. 3409(a).

[38] It is fairly clear that financial institutions providing wire transfer services to their customers would constitute "electronic service providers" under ECPA, in part relying on the breadth of the definition of "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. 2510(12). The legislative history seconds this surmise, in setting forth as an example of electronic communication, "funds transfer among financial institutions." S. Rep. No. 99-541, 99th Cong., 2nd Sess. 1, 8 (1986).

Although banks might not view themselves as "electronic service providers," ECPA would appear to, even though banks may rely upon leased telephone lines to actually conduct the electronic communications. Similarly, bulletin board services and other e-mail providers rely upon existing communication facilities, but are covered by ECPA as "electronic service providers."

[39] One of the better counterarguments to this conclusion that ECPA covers wire transfers derives from a fragment of legislative history, noting that "[c]ommon computer-to-computer communications include the transmission of financial records or funds transfers among financial institutions. . . . " S. Rep. No. 99-541, at 99th Cong., 2nd Sess. 1, 8. This might be viewed as giving rise to the shaky inference that ECPA binds only *financial institutions* providing communications services, leaving a non-financial institution such as CHIPS or the Fedwire system beyond its purview. This conclusion is not warranted, because the legislative history cited does not purport to provide a comprehensive and exclusive definition of "computer-to-computer" communications; rather it is only setting forth a non-exhaustive laundry list of modern electronic communications. In any case, *Steve Jackson Games, op. cit.,* footnote 34 , supports the proposition that acquisition of stored electronic mesengers in transit to the intended recipient violates title II of ECPA.

[40] 18 U.S.C. 2703(a) and (b).

## BOX 5-3: Legal Mechanisms for Acquiring Records

- *Administrative* subpoena—exercised by executive agencies pursuant to an express grant of subpoena power for enumerated purposes; forces the production of records already maintained.
- *Grand jury subpoena—a* significant tool for criminal investigations, signed by foreman of grand jury; must be relevant and material to a matter properly before the grand jury. 18 U.S.C. 3321; Fed. R. Crim. P.6.
- Search, *seizure and arrest* warrants—supported by probable cause and signed by a magistrate, as required by the Fourth Amendment.
- *Court order—a* legislative requirement, such as Title II I three judge panel court orders sanctioning wiretapping.
- *Trial subpoena*--- available once a defendant has been indicted by a grand jury finding probable cause that defendant committed a crime; no judicial intervention required of prosecution in obtaining further subpoenas,

SOURCE: Office of Technology Assessment, 1995

toring of the communications for discovering criminal conduct and informing law enforcement would be illegal.[41,42]

Many commentators have extolled the virtue of moving toward coherent and synoptic legislation in the area of privacy law, and certainly wire transfer monitoring legislation would provide an opportunity to rationalize the field and perhaps avoid conflict with the growing European movement towards comprehensive data protection. For the purposes of enabling a wire transfer monitoring system to go forward, however, revisions must be made to RFPA, ECPA, and perhaps the Privacy Act. Nevertheless, policy is poorly made fragment by fragment, a problem stemming from institutional vacuum, i.e., the United States has no centralized privacy agency which might otherwise shape a privacy agenda and provide guidance on the host of issues arising at the intersection of new technology and individual privacy.[43]

Independent of what interpretation of ECPA and RFPA will prevail, financial institutions deserve regulatory certainty, hence any monitoring proposal should clearly delimit financial institution obligations and provide safe harbor from suits. Financial institutions are properly concerned with civil suits from both the government, for failure to comply with regulatory requirements such as the BSA and suspicious transaction re-

[41] 18 U.S.C. 2702(b)(6). A similar provision is found in the contemporaneous interception provisions of Title I of ECPA (codified at 18 U.S.C.2511 (3)(b) (iv)) and permitting the disclosure of the contents of a communication if inadvertently obtained by the service provider and if pertaining to criminal conduct. See also, S.Rep. No. 99-541, 99th Cong., 2d Sess. 1, 26 ("If the provider purposefully sets out to monitor conversations to ascertain whether criminal activity has occurred, this exception would not apply" and the service provider would be criminally liable for disclosing the content of the communication).

[42] A final relevant provision states that in order to obtain a court order for information in an electronic communications system, a government agency must show that there is reason to believe the contents of the communication are relevant to a legitimate law enforcement inquiry. 18 U.S.C. 2703(d). This provision suggests how contrary to ECPA's intent this proposal would be, unless Congress deems that all wire transfer communications are relevant to law enforcement's mission.

[43] OTA has long noted the policy arguments supporting the establishment of some form of privacy ombudsman, most recently in the report *Information Security and Privacy in Network Environments.* U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994).

porting,[44] and from customers, who may sue under RFPA for improper disclosures of financial information. Consequently, a paramount consideration is the minimization of financial institution liability for complying with any wire transfer reporting requirements.

With the Annunzio-Wylie Anti-Money Laundering Act of 1992, Congress enacted a comprehensive "safe harbor," or immunity from customer suit for banks disclosing customer information under suspicion transaction reporting or other requirements.[45] While the current language is quite broad[46] it may be necessary to clarify that the safe harbor provision covers disclosures of wire transfer records where there is little or no basis for believing that a customer might be engaged in criminal conduct, or where pre-determined guidelines are followed, as in technical option 4 (see chapter 7). ECPA contains a safe harbor as well, providing that any disclosure of electronically stored communications does not give rise to civil or criminal liability, as long as the disclosure was in good faith reliance upon a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization.[47]

To minimize the intrusiveness of a wire transfer monitoring system, an administrative regime might be set up to require human confirmation of any positive "hit" before more intrusive traditional law enforcement techniques are applied. This would assure that targets misidentified by false positive hits do not have their right to seclusion unnecessarily disturbed.[48] Under such a system, a human operator would intervene and search for confirming evidence, before authorizing intensified scrutiny, as part of graduated progression of escalating surveillance. As a further protection against unwarranted intrusions into innocent conduct, the process might grant notice to the targeted party, although this notice should be carefully circumscribed to prevent tipping off malefactors. Of course, the intervention of a human operator carries negative effects, as well, raising the possibility of official misconduct and unauthorized access.[49] A priority in crafting a balanced system would be the inclusion of security safeguards to limit unauthorized browsing, as well as guidelines to limit official discretion and to protect against arbitrary and capricious action. At the same time, discretion can also operate as a safety valve, in permitting agents the latitude to terminate investigations without merit before any damage is done to innocent parties.

---

[44] 12 U.S.C. 5313(g). RFPA, at 12 U.S.C. 3413(d), specifically states that nothing in RFPA "shall authorize the withholding of financial records or information required to be reported in accordance with any Federal statute or rule promulgated thereunder." Hence, financial institutions are obligated above all to comply with government dictates, with the potential of leaving them exposed to civil liability.

[45] Pub. L. 102-550, section 1517, 106 Stat. 4059-4060, codified at 12 U.S.C. 3413(g)(3). The provision states that "[a]ny financial institution that makes a disclosure of any possible violation of law or regulation or a disclosure pursuant to this subsection or any other authority . . . shall not be liable to any person . . . for such disclosure . . . ."

[46] "Safe harbor" provisions do not deter the bringing of suits, however, a continuing source of bank concern. *See,. e.g.*, *MacLean* v. *Riggs Nat'l Bank*, (No. 94-0259-CRR, D.D.C. 1994)(plaintiff suing bank for a breach of RFPA, where plaintiff had defrauded bank and bank had reported crime to federal authorities).

[47] 18 U.S.C. 2707(d).

[48] The Supreme Court recently spoke to the issue of false positives in the computing context in *Arizona* v. *Evans*, where a computer erroneously indicated the existence an outstanding warrant on Isaac Evans, resulting in his false arrest and subsequent conviction on unrelated charges. (Docket No. 93-1660, March 1, 1995). While a 7-2 majority ruled to uphold the arrest because the police were acting in good faith reliance on the computerized records, five justices signaled their concern for the dangers of computer errors and loss of liberty. Significantly, the majority opinion relied upon the fact that judicial personnel, not law enforcement, were culpable in the computer error. Perhaps, a court will be disinclined to follow the *Evans* precedent where law enforcement itself was to blame for computerized errors.

[49] For this reason, some privacy advocates object least to a "black box" system, which would assess each wire transfer on the fly against a profile of money laundering attributes, discarding all those transfers not meeting the profile. OTA Workshop on Privacy and Confidentiality, September 28, 1994.

## THE PRIVACY OF THE INDIVIDUAL AND THE CONTROL OF CRIME

> No law can ever be made but what trenches upon liberty: if it stops there, it is so much pure evil: if it is good upon the whole, it must be in virtue of something that comes after. It may be a necessary evil: but at any rate it is an evil. To make a law is to do evil that good may come. J. Bentham, *Of Laws in General*, H.L.A. Hart, ed. (London: Athlone Press, 1970), chapter VI, 4, p. 54.

Few wire transfers are initiated by individuals, in relation to the total number and dollar volume of wire transfers.[50] Consequently, commentators concerned about individual privacy in payment systems have focused on consumer transfer systems, which include automated clearing houses (ACHs), automated teller machines (ATMs), point-of-sale and other forms of electronic debiting transactions.[51] Consumer transactions contain a wide variety of information, potentially indicating individuals' spending habits, lifestyles, and locations, as well as political and religious expressions. The sort of information that may be harvested from these types of transactional records would be rather distinct from the kind of information in wire transfer records, even with respect to the natural persons using the wire transfer apparatus.[52] And while consumer transactional information may be interesting to law enforcement's control of money laundering, the proposed monitoring systems would only analyze wire transfers over wholesale payments systems.

Although the current wire transfer system is predominantly a corporate instrument, there may be momentum to individual or closely held corporate use of the wire transfer.[53] Emerging forms of electronic payment, such as digital money (see box 7-4 in chapter 7) may serve the needs of individuals for immediate payments over networks. If so, then the intrusion of a monitoring system on individuals' or even corporations' privacy would be slightly mitigated by the existence of a more secure and equally efficient alternative. But this line of analysis may be begging the question, if the monitoring of funds transfers serves as a precedent for government monitoring of digital money systems. The threat of the slippery slope may be somewhat overstated, however, in light of the very different character of wholesale wire transfer systems and consumer systems, the latter of which already enjoy considerable legal protections.

---

[50] Telephone interview with Ed Regan, Vice President, Chemical Bank, August 16, 1994; interview with John Byrne and Kawika Daguio, American Bankers Association, August 4, 1994. Although law enforcement would putatively be looking at corporate transactions, one of the intended results is the prosecution of individual money launderers, along with the punishment of criminally tainted corporations by revocation of charters and fining corporations to the extent of their assets. Thus, the system could potentially circumvent the panoply of procedural requirements protecting the individual. *Boyd* v. *United States* may still speak to this question, as the facts of the case are somewhat analogous, with law enforcement targeting individuals by searching corporate documents without probable cause. 116 U.S. 616 (1886) ("illegitimate and unconstitutional practices get their first footing . . . by . . . slight deviations from legal modes of procedure").

[51] These transactions are covered by the Electronic Funds Transfer Act of 1978 (EFTA)(Pub. L. 95-630), codified, as amended, at 15 U.S.C. §1693 *et seq*. EFTA, and its implementing Regulation E, which provide privacy and other protections to electronic funds transfers connected to consumer accounts, accounts "established primarily for personal, family, or household purposes." 15 U.S.C. §1693a(2). All funds transfers through Fedwire, however, "even those involving consumer accounts, are exempt from EFTA and Regulation E." E. Patrikis, T. Baxter, and R. Bhala, *Wire Transfers*: *A Guide to U.S. and International Laws Governing Funds Transfers* (Chicago, IL: Bankers Publishing Co., 1993), p. 147. An interesting thought deriving from this last statement would be that individuals already use the wholesale funds transfer system at their own peril and assume the rules of its game, including perhaps, future monitoring for money laundering.

[52] The American Bankers Association demurs slightly, in observing that the wire transfer messages of individuals, often relating to small dollar cash transaction or investment activities, may contain highly personal information and instructions relating to specific investments and business transactions.

[53] Citicorp offers the WorldLink product, a gateway for small business use of the wire transfer system. Increasingly, big banks are able to offer on-line access to the wire transfer system to their clientele, bringing the marginal costs of wire transfers down dramatically.

## Conceptualizing the Intrusion

### *The Initial Access Question*

Marx and Reichman have argued that where the subject of a search is unaware of the search, where neither direct nor willing consent has been given to a search, the search is more intrusive.[54] This secret surveillance is believed to be particularly intrusive if the subjects are not given notice that they are a "positive hit," or thought to be suspect. Although these judgments were developed in the context of computer matching to detect fraud in entitlement programs, they might also be applicable to asset seizure, where the presumption of innocence is transformed into asset holder's affirmative duty to disprove the connection to illegal conduct.

### *The Subsequent Manipulation of the Data and the Problem of False "Hits"*

While some argue that any secondary use of wire transfer information should be strictly controlled, a greater concern arises once a positive "hit" is generated and acted upon. At this point, the concern is one of the damage, economic or otherwise, visited upon the innocent party unjustly brought under suspicion by a false positive "hit," an occurrence that can be expected to be common for any wire transfer monitoring system.[55] Errors arising out of computer matching systems have been categorized as falling into two broad classes: 1) flaws in the computing/data entry system; and 2) flaws in attempting to reduce analysis to a rule-based system, what Marx and Reichman term the "acontextual nature" of computer reasoning. Both flaws may result in false positive "hits," although the first group should become progressively smaller (but never to disappear entirely) as computing technology improves.

The first group breaks down further into erroneously reported or entered data; obsolescence of information from initial entry; and computer hardware/software errors. The latter group has been identified by Marx and Reichman to be the "acontextual nature of the decision process, and the probabilistic nature of profiling" (i.e., coincidences of profiling). The latter errors would be expected to arise repeatedly when a profile is used to separate licit and illicit wire transfers on the basis of the sketchy information contained in the wire transfer. For instance, threshold clearing accounts, described in chapter 1, are a standard business practice, yet also resemble money laundering schemes. Also, the profiles are likely to be skeletal, hence many innocent people can be expected to meet the profile by pure coincidence. Additionally, law enforcement has no baseline figures for what the proper ratio of positive to negative should be, nor, in fact, can law enforcement be certain that all money laundering schemes are incorporated into the profile—knowledge is distorted by the detected criminals, who are ipso facto less competent than their unapprehended money laundering cohorts.

What are the costs to targets falsely labeled as suspicious? Presumably, investigations will intensify, with intrusive, albeit legal tools of modern law enforcement. One could expect that businesses, in particular, could suffer deleterious economic consequences should the law enforcement

---

[54] Gary T. Marx and Nancy Reichman., "Routinizing the Discovery of Secrets," *American Behavioral Scientist*, (March/April 1984), pp. 423-52, 440. But disclosure of a search may often vitiate the law enforcement mission: consider the U.S. Customs Service's practice of having dogs sniff international luggage in transit before passengers claim their bag. Otherwise, if a dog "alerts" to narcotics in a bag, the narcotics trafficker would be expected to abandon the bag, leaving the agents with the contraband but not the miscreant.

At least one expert from the law enforcement community disagrees with the proposition that undisclosed non-retained screening compromises privacy. Telephone interview with Scott Charney, Chief, Computer Crime Unit, Department of Justice. Consider also the aforementioned case of *Steve Jackson Games* and the constitutional obligation to avoid the seizure and review of the contents of communications not relevant to a law enforcement inquiry. 36 F.3d at 463. The court observed that computerized key word searches of unread e-mail to filter out irrelevant or innocuous messages decreased the risk of improper access to innocuous communications.

[55] See chapter 4, box 4-5, for a fuller discussion of the problem of false positive in settings with low incidence of the conduct being sought.

scrutiny become public.[56] A further detriment to the computer "hit" could be a shift in the presumption of guilt, in the sense that a computer can precipitate the seizure of assets.[57]

## Balancing the Interests of Law Enforcement and the Individual

### *The Changing Balance of Power Between Criminals and Law Enforcement*

As criminals become increasingly sophisticated and take advantage of new technology, crime itself becomes less apparent, particularly so with "victimless" crimes such as money laundering. In the case of wire transfers, the money launderers conceal their activity in the stream of commerce. Law enforcement argues that if it may not legitimately scrutinize the electronic stream of commerce for wrongdoing, criminals will go undetected and unpunished.

Sometimes technology greatly aids law enforcement's mission, such as computerized databases available for instantaneous records checks and computerized fingerprint analysis. But at the same time, emerging technologies like public key encryption and digital telephony may undermine law enforcement efforts. Will law enforcement be permitted to shape (and perhaps pay for) the structure of technological development to keep the balance of power between law enforcement and the criminal element status quo or to tip the balance in society's favor? At the same time, technology may offer the best of both worlds, sheltering privacy while permitting increased investigative powers. This could permit anonymous payments until certain objective criteria are satisfied, established either by legislative or administrative regime and justifying access to the wire transfer.

This argument regarding the balance of power between law enforcement and the criminal may be irrelevant. The criminal is relying upon electronic technology for the execution of the crime of money laundering. This distinguishes a wire transfer monitoring system from the usual scenario, where the increased intensity of electronic surveillance would shift the balance of power between the state and the scrutinized in permitting electronic technology to manipulate data in ways that paper could not be analyzed. In a sense, criminals are benefiting from technology and exposing themselves to detection at the same time.

### *The Costs of Traditional Law Enforcement Techniques*

What are the costs of traditional law enforcement techniques where the traditional citizen-reporting model for detecting offense is not tenable?[58] Given the near invisibility of money laundering, particularly past the placement stage, law enforcement has relied heavily upon undercover operations in trapping money launderers,[59] raising the specter of, at best, police complicity in permitting money laundering to go forward in order to build a case, with a strain on limited police resources to conduct storefront operations; or at worst, entrapment and police corruption. Consider also the French example: TracFin, the French

---

[56] If a corporation is publicly suspected of narcotics trafficking or money laundering, in all likelihood its banks will cut off banking relations lest the banks later be accused of complicity in further money laundering. Of course, many other examples of economic harm may be readily imagined—vendors demanding cash upon delivery out of a concern for future legal problems, and so on.

[57] Marx and Reichman, op cit., footnote 51, p. 441. Privacy advocates favor followups to positive hits before entitlement program benefits are cut off. "[T]o protect due process and Constitutional rights, however, this effort [to computer match and save money] should also involve detailed and, where necessary, extensive followup efforts." David F. Linowes, *Privacy in America: Is Your Private Life in the Public Eye?* (Urbana, IL: University of Illinois Press, 1989), p. 95. In all likelihood, any computer "hit" would be buttressed by independent evaluations to form reasonable suspicion before a seizure is effected.

[58] One lost asset of citizen reporting is its inherent ability to circumscribe police discretion, hence other means to control discretion must be sought out in the case of electronic surveillance. Marx and Reichman, "Routinizing Surveillance," *op. cit*, footnote 54, p. 423. See, generally, Gary T. Marx, *Undercover: Police Surveillance in America* (Berkeley, CA: University of California Press, 1988).

[59] In fact, the money laundering criminal statute had to be redrafted soon after its initial enactment to accommodate sting operations.

intelligence agency which is a near analog to the United States' FinCEN (see chapter 3), relies on a network of informants within the banks themselves to report suspicious activity by phone or fax.[60] Perhaps most interesting for the current analysis are the secrecy "agreements" that the informants enter into with TracFin, wherein they promise not to reveal their communications with TracFin to their fellow bank employees. The costs of trying to enforce money laundering statutes without recourse to computer surveillance would be an increased amount of human surveillance and spying within the banking system itself (with difficulties in limiting the scope of the human surveillance to the immediate task of ferreting out money laundering).

## The Control of Government Over Society

Some commentators associate increasing social control with conformity and a loss of individuality.[61] Others counsel against the irreversible trend of systems of government towards more intensive and extensive social control. Marx notes that law enforcement, like all apparatuses of social control, tends toward increasing rationalization, in seeking to be more effective, efficient, certain and predictable.[62] Many privacy commentators have adopted and adapted Bentham's concept of the panoptic eye, originally scrutinizing the incarcerated for purposes of controlling prisons, but now turned outward regarding all citizens and their transactions with suspicion, measuring their conduct against a backdrop of criminality.[63] Some social scientists qualify this panoptic argument, stating that evidence for changed behavior in the face of perceived surveillance must be seen, before inferences of tyrannical social control may be drawn.[64]

Interestingly, the BSA reporting requirements present an example of the often paradoxical response of society to a new attempt at social control. After law enforcement's wakeup call to the banking community as well as the criminal element with Operation Greenback and the Bank of Boston case (see chapters 1 and 3), the phenomenon of smurfing arose, as money launderers sought to discover a new invisible path into the financial system. The behavior of miscreants has changed, but little is known about whether legitimate cash transactors have changed their behavior, whether government control has adversely influenced the innocent individual.

The control of crime is central to the functions of modern governments, in the maintenance of a stable social order. The sovereignty of the state may be at stake, in its inability to control money across borders and protect the integrity of its cur-

---

[60] Interview with Joseph Myers, Asst. Legal Counsel of FinCEN; TracFin's 25 agents work with about 4,000 "correspondents," one in each of financial institutions, reporting about 60 tipoffs each month. Monaco has recently set up an analogous agency, Siccfin, to follow dirty money. "Monaco acts to cut down dirty laundry," Andrew Jack, *Financial Times*, October 25, 1994, p. 2.

[61] See, e.g., Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser," 39 *N.Y.U. L. Rev.* 962, 1003 (1964)("The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass.")

[62] Marx and Reichman, *op. cit.*, footnote 54, p. 442. Marx also observes that any dramatic shift towards a totalitarian state would likely occur "by accretion [rather] than by cataclysmic event." Marx, *Undercover*, *op. cit.*, footnote 55, p. 229. Whether wire transfer monitoring would represent a significant "accretion" would likely hinge on the legislative regime authorizing the monitoring.

[63] For instance, Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, CO: Westview Press, 1993). In other writing, Marx notes that "mass" surveillance violates the spirit of the Fourth amendment, "because the burden of proof is shifted from the state to the target of the surveillance," upending the traditional American tenet of innocence until proven guilty. Marx, *Undercover*, *op. cit.*, footnote 58, p. 227.

[64] See, e.g., David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis, MN: University of Minnesota Press, 1994). Lyon casts a skeptical eye at blanket assertions that technology inevitably enhances the power of organizations over the surveyed population. p. 166.

rency. The state's decision regarding what to criminalize lies at the heart of sovereignty, a decision increasingly undermined by the impunity with which the money launderer moves money across international borders.

## Unanticipated Consequences of a Monitoring System

Many commentators note the leveling effect of computer analysis of records: in a sense, everyone's privacy is violated blindly and equally.[65] Nevertheless, law enforcement enjoys considerable discretion in deciding which leads merit further investigation, allowing discretion back into the equation. Marx and Reichman note this in stating that

> "[t]he discovery of infractions, of course, is only the first stage in the enforcement process. . . . An overabundance of cases and disinterest, or bias on the part of the enforcement agent, may result in no action being taken." page 447, footnote 13.

Of course, governmental followup to positive matches is often considered salutary, and in fact is mandated by the Computer Matching and Privacy Protection Act of 1988,[66] though this comes in the context of required corroboration before government benefits may be cut off on the basis of a positive hit.

At the same time commentators frequently note that all the repercussions of new computer systems may not be readily and accurately anticipated. Burnham, in his influential *The Rise of the Computer State*, details repeated instances of computer systems being used for purposes quite different than their architects planned.[67] A recent example of this would be the video surveillance of public squares in English towns: instead of helping in the apprehension of violent criminals, the human monitors of the video cameras have come to observe and report parking meter scofflaws and litterers. David Lyon interprets Burnham's views even more darkly: Lyon suggests that new computer technologies augment themselves beyond the direct control of anyone.[68]

Perhaps most speculatively, the deleterious impact of the "electronic informant" on the legal system may be raised. At least one commentator, a former federal prosecutor, has questioned the uncritical receptiveness of lawyers and judges to computer evidence, a confidence he feels is misplaced, in advocating increased scrutiny of computer-generated evidence and testimony at trial. Other commentators have extolled the benefits, including uniformity, of aiding the magistrate in her determination of probable cause for search and arrest warrants, through the use of expert systems.[69]

---

[65] Both García and Marx and Reichman observe this, particularly when compared to the biases inherent in citizen reporting as the sole means for identifying suspects. Robert García, "'Garbage In, Gospel Out': Criminal Discovery, Computer Reliability and the Constitution," 38 U.C.L.A. L. Rev. 1043-1145 (1991); Marx and Reichman, *op. cit.*, footnote 54, p. 442. Consider also *Sitz*, and the emerging theory that the Fourth Amendment only guards against arbitrary distinctions in the level of scrutiny and surveillance rather than providing an absolute floor of protection against state scrutiny.

[66] 5 U.S.C. 552a(a)(8)(B)(iii) specifically exempts law enforcement agencies from the provisions of the Computer Matching Act. The Federal Privacy Act also exempts law enforcement from many of its provisions. 5 U.S.C. 552a(j)(2). At the same time, the Privacy Act's section 552a(o) governs the transfer of databases from one agency to another for matching, and could potentially impact a non-law enforcement agency's downloading information to FinCEN.

[67] David Burnham, *The Rise of the Computer State* (New York, NY: Random House, 1983).

[68] Lyon, *op. cit.*, footnote 64, p. 11.

[69] Christopher J. Moran, "A Neat Set of Legal Rules: Improving the Search Warrant Decisionmaking Process Through Guideline Implementation," submitted to Professor Henry H. Perritt, Jr., Villanova University School of Law (May 11, 1992). Available on the World Wide Web (July 19, 1995) at: gopher://ming.law.vill.edu:70/00/.ftp/pub/law/search.warrant/.files/Search.Warrant.txt

## THE CONFIDENTIALITY INTEREST OF THE CORPORATION

### A Short Legal History of the Corporation in America

In the early years of the United States, legislatures granted charters to corporations so that they might serve a public purpose in exchange for a monopoly right, ordinarily, the right to operate a turnpike or bridge, thus encouraging development in a capital-poor environment. This relationship of the legislature and corporation led to Justice Marshall's famous language in *Trustees of Dartmouth College* v. *Woodward*, where he observed that the corporation is "an artificial being, existing solely in contemplation of state law."[70] Nuances aside (such as the fact that corporations are created pursuant to state law and would be regulated by federal law for present purposes), the "artificial being" theory places few, if any, restrictions upon governmental actions affecting the corporation, implying that the corporate interest in confidential payments may be subordinated to the state's interest in policing money laundering.

Defenders of corporations argue that this theory is flawed, in light of the dramatic changes in the process of incorporation, as well as the ability to shop among the states for advantageous incorporation laws and the greatly reduced mandatory requirements for incorporation. They submit that the contractual theory of the nature of corporations, namely the use of contracts to minimize the problems associated with the separation of ownership and control in the modern corporation, has risen to the fore, rendering misplaced judicial and legislative reliance on vestiges of the "artificial being" theory.[71] Butler and Ribstein argue that government regulation should not interfere with the set of contractual relationships that constitute the modern corporation; however, it is unclear how far this argument may extend in the context of law enforcement. In this limited context, the presumption in favor of the state's interest in preserving law and order by detecting and punishing money laundering may permit regulation in the form of mandated disclosure of hitherto confidential payments information.

Although the *Lochner*-era and *Slaughterhouse* cases—the high-water mark of the corporation's successful invocation of the Constitution to nullify legislative regulation—ended in 1937, the modern Supreme Court has gradually, if haltingly, enhanced the corporation's status under the Constitution, even though the Constitution makes no mention of the corporation, only persons. [72] The nadir of corporate rights is represented by the *Morton Salt* decision, a late revival of the "artificial entity" theory, rejecting a corporate right to privacy.[73] While denying the general principle of corporate personhood, the Court noted that corporations "may and should have protection from unlawful demands made in the name of public investigation." Nevertheless, the Court upheld the Federal Trade Commission's access to corporate records, citing to an earlier case, where the gov-

---

[70] 17 U.S. (4 Wheat.) 518, 636 (1819). *United States* v. *Morton Salt Corp*, 338 U.S. 632 (1950), represents a late revival of the "artificial entity" theory.

[71] See, e.g., Henry N. Butler and Larry E. Ribstein, *The Corporation and the Constitution* (Washington, DC: The AEI Press, 1995), pp. ix - x, 18-22. One of the linchpins of this argument is the fact that corporations are no longer chartered by legislatures, rather incorporated by "perfunctory" state filings. Even if this historical shift in the manner of incorporation is regarded as dispositive, it is not apposite for the matter of banks, which continue to receive ornate charters specifying obligations and waivers of rights. As a result, the bank itself would be infirm in arguing that it deserves relief from the law enforcement regulations integral to the monitoring of wire transfers.

[72] Specifically, corporations invoked the protections of the 14th amendment to nullify early state health and safety regulation of the corporation.

[73] *United States* v. *Morton Salt Corp.*, 338 U.S. 632 (1950).

ernment was allowed to rummage through corporate documents on no more than an "official's curiosity."[74]

In the wake of *Morton Salt* the Supreme Court has by fits and starts extended the protections of the Bill of Rights to corporations, rendering the Constitution "a potent shield against government regulation."[75] For instance, the Court has recognized the corporation's right to invoke a limited measure of First Amendment protection for its advertising.[76] The landmark case of *First National Bank of Boston* v. *Bellotti* extended the right of political speech to corporations, although later rulings of the Court have softened *Bellotti* somewhat. [77]

Most relevant to the proposed monitoring system, the Supreme Court has extended weakened Fourth Amendment protections to the corporation. *Marshall* v. *Barlow's Inc.* struck down as unconstitutional a provision of the Occupation Safety and Health Act authorizing warrantless workplace inspections. This ruling brought some of the protections of the Fourth Amendment to commercial buildings, beyond the core Fourth Amendment solicitude for the home as castle.[78] One commentator theorizes that the decision "represented the protection of New Property—information about workplace operations that the corporation sought to conceal from government—and it demonstrated the importance of the intangible Bill of Rights [of association, privacy and speech] in the modern political economy."[79] *Morton Salt* itself cautioned against "fishing expeditions," or government searches of ordinary business records to detect illegitimate conduct,

---

[74] The Court noted that "even if one were to regard the request for information [a complete set of terms and prices for products] as caused by nothing more than official curiosity, nevertheless law-enforcing agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with law and public interest." 338 U.S. at 652. The Court went on to note, however, that "[o]f course, a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power." (citation omitted.)

[75] Carl J. Mayer, "Personalizing the Impersonal: Corporations and the Bill of Rights," 41 *Hastings L. Rev.* 577-667, p. 661 (March 1990). Mayer catalogs successful corporate invocations of the Bill of Rights—First Amendment guarantees of political speech, commercial speech, and negative free speech rights; Fourth Amendment safeguards against unreasonable regulatory and other searches; Fifth Amendment double jeopardy and liberty rights; and Sixth Amendment entitlement to jury trial. *Ibid*., appendix I, pp. 664-65. Corporations have met with success in advancing Eighth Amendment arguments as well, particularly the excessive fines clause.

[76] *Pittsburgh Press Co.* v. *Human Relations Commission*, 413 U.S. 376 (1973)("commercial speech" or advertising receiving diminished protection relative to individuals' speech).

[77] No ideology possesses a monopoly on the charter theory of the corporation: Justice Rehnquist, in dissenting on *Bellotti*, cleaved to the *Dartmouth College* theory of the corporation, in noting that a corporation "possesses only those properties which the charter of creation confers on it, either expressly, or as incidental to its very existence." 435 U.S. 765, 823 (Rehnquist, J., dissenting), quoting *Dartmouth College*, 17 U.S. (4 Wheat.) at 636. Another dissenter, Justice White, makes the interesting point that a corporation should enjoy First Amendment protections only where it furthers self-expression by the shareholders. *Bellotti*, at 805. See also, Butler and Ribstein, *The Corporation and the Constitution*, *op. cit.*, footnote 71, pp. 61-2.

[78] *See* v. *City of Seattle* also granted commercial premises Fourth Amendment protection, although the administrative warrant required will be measured not against probable cause that a violation has occurred, but rather against "a flexible standard of reasonableness that takes into account the public need for effective enforcement of the particular regulation involved." 387 U.S. 541, 545 (1967); see also *Camara* v. *City of Seattle*, 387 U.S. 523, 534-39 (1967)(adminstrative warrants must be reasonable and tightly tied to a legitimate government purpose, but need not be based on probable cause that a particular building is in violation of fire code regulations). The *See* Court also noted other cases where the Supreme Court refused to uphold criminal investigative searches violative of the Fourth Amendment simply because the illegal searches occurred on commercial rather than residential premises. 387 U.S. at 543.

[79] Mayer, "Bill of Rights," *op. cit.*, footnote 73, p. 609. Mayer goes on to question the merits of according intangible rights to a non-person, particularly under the Fourth Amendment with its embedded privacy right. *Ibid.*, p. 643-45. Mayer does not contest the propriety of according constitutional protection to corporate *property.*

but later cases have upheld very broad subpoenas.[80]

The more recent companion cases of *Ciraolo*[81] and *Dow Chemical*[82] turned on the same Fourth Amendment issue—whether aerial overflights of defendants' property constituted "searches" requiring probable cause and warrant—using identical analyses, despite the fact that the target of the overflight in one case was a natural person's backyard and the other a corporation's industrial plant. One might infer from these cases, decided on the same day, that the Fourth Amendment is now blind to the distinction between artificial and natural persons. In fact *Dow Chemical* is noteworthy for the absence of a discussion of the status of corporate entities under the Fourth Amendment.

## What Is The Basis for a Corporation's Right to Confidentiality?

Judge Posner would accord the corporation a stronger privacy right than the individual. Posner is concerned that threats to the confidentiality of business information will erode the profit incentive informing entrepreneurial risk-taking. Noam and Greenawalt corroborate this view from a different perspective: they note that "arguments for confidentiality by business organizations must be cast in terms of the functioning of social institutions, and most of the arguments rest on assumptions about economic efficiency."[83] If the utility of corporate confidentiality is the overriding policy concern, then the analysis must devolve into the question of the legitimate needs of corporate confidentiality in payment systems information.

Others might argue that the rights of the corporation might emanate from the collective rights of the underlying individuals. This libertarian concern grows where the artificial entity is a closely held corporation or small partnership. Support for this viewpoint is supplied by RFPA, in its protection of corporations and partnerships with fewer than five members: as the size of corporation diminishes, the identities of those comprising it become more transparent and their *privacy* interests as members of the corporation or partnership swell. Professor Anita Allen suggests other bases for according corporations privacy rights: "the moral status of the corporation as a social participant [*i.e.*, society imposes burdens on the corporation such as taxation, liability for injuries and losses caused] demands that its 'equivalent injuries' [loss of privacy] be compensable; and that social justice demands the fullest protection of corporate privacy no less than of individual privacy."[84] This moral ground for a right to corporate privacy is at least partially undercut by Milton Friedman's seminal "The Social Responsibility of Business is To Increase its Profits,"[85] which maintains that the corporation does not bear responsibi-

---

[80] *Morton* Salt, 338 U.S. at 642; Eli Noam and Kent Greenawalt, "Confidentiality Claims: Glittering Illusions or Legitimate Concerns?" *Business Disclosure: Government's Need to Know*, Harvey J. Goldschmid (ed.)(New York, NY: McGraw-Hill, 1979), pp. 378-418, p. 387, *citing Federal Trade Commission* v. *Crafts*, 355 U.S. 9 (1957) and *Civil Aeronautics Board* v. *Hermann*, 353 U.S. 322 (1957).

[81] *California v. Ciraolo*, 476 U.S. 207 (1986).

[82] *Dow Chemical Co.* v. *U nited States*, 476 U.S. 226 (1986).

[83] Noam and Greenawalt, "Confidentiality Claims," *op. cit.*, footnote 80, p. 382-83. Economic efficiency parses as questions subject to empirical study, such as "will an industry be made less or more competitive?" "[w]ill the burden of producing the information outweigh the likely benefits of its being produced?" "[i]f the overall 'economic' effect of disclosure of the information is likely to be negative, does some other justification. . .support its being revealed?"

[84] Allen, "Corporate Privacy Rights," *op. cit.*, footnote 12, p. 638. Mayer makes the opposite point, that the corporation benefits too much from the current legal structure—on one hand endowed with limited liability for some industrial accidents, the use of voluntary bankruptcy and perpetual life, "creating unaccountable Frankensteins that have superhuman powers but are nonetheless constitutionally shielded from much actual and potential law enforcement. . .." Mayer, "Bill of Rights," *op. cit.*, footnote 73, pp. 658-59.

[85] Milton Friedman, "The Social Responsibility of Business Is To Increase its Profits," *Business Ethics: Corporate Values and Society*, Milton Snoeyenbos, Robert Almeder and James Humber (eds.)(Buffalo, NY: Prometheus Books, 1983), pp. 73-79.

lities to society other than a duty to maximize the shareholders' stake in the corporation. Vietnam-era shareholder lawsuits seeking to inform corporate decisionmaking with values other than profit maximizing met with a similar judicial conclusion.

## The Subjective Expectation of Confidentiality in Corporate Communications

Corporations often negotiate separate confidentiality accords with banks conducting wire transfers on their behalf.[86] A Chicago-based Citibank subsidiary providing wire transfer services to small businesses relates how some corporate clients require them to sign confidentiality riders barring release of the information contained in wire transfers, even though their standard service agreement already contains nondisclosure clauses. Other corporations may not, relying perhaps upon an implied right of confidentiality in the customer/bank relationship[87] or simply expecting confidentiality due to the longstanding tradition of banks to maintain customer confidences.[88]

There are considerable legitimate grounds for corporations to desire secrecy in wire transfers and to fear disclosure to competitors. Sensitive information would include the size and timing of payments to legal counsel, major stock transactions,[89] payroll information, identities of and prices paid to suppliers of inputs, as well as evidence of cost structure, generally. All this information could be derived from wire transfer records, particularly because corporations, already paying a flat fee for the wire transfer service, may use empty fields within the wire transfer messages to communicate additional information.[90] If this information is useful to law enforcement, there might be information in the stream of payments similarly valuable to aggressive competitors, industrial spies and would-be defrauders of the corporation[91] (see box 5-4). At the same time, the same paucity of information on the wire transfer record that threatens the utility of any monitoring proposal (see, in particular, chapter 4)

---

[86] Vicki Roberts, Treasurer, Centex Corporation, Houston, Texas, at OTA Workshop on Privacy and Confidentiality in Payment Systems, September 28, 1994.

[87] Fischer, *The Law of Financial Privacy, op. cit.*, footnote 15, ¶7.04. The state of New York adopted this doctrine in *M.L. Stewart & Co.* v. *Marcus*, 207 N.Y.S. 685, 691 (Sup.Ct. 1924), *aff'd* 228 N.Y.S. 856 (1927). While the implied duty or contract is fairly well settled in the United States, the scope of the duty has not been fully resolved as to whether the duty of confidentiality extends beyond the depositor relationship. p. 7-15.

[88] An absolute trust in banks might not be well-placed: while banks plead the customer's expectation of privacy in the banking relationship, banks "may claim a qualified privilege against further lawsuit [defeating a privacy tort claim for disclosure of confidential communication] when [the banks] disclose accurate customer account information to another bank." Smith, *The Law of Privacy in a Nutshell, op. cit.*, footnote 13, citing *Graney Development Corp.* v. *Taksen*, 92 Misc.2d 764, 400 N.Y.S.2d 717, *aff'd* 411 N.Y.S.2d 756 (1978).

[89] Note the parallel to early wiretaps on telegraph lines, executed by parties attempting to eavesdrop upon stock tips and other sources of financial information.

This example suggests another analogy for wire transfer monitoring, the self-regulatory organizations (SROs) and their surveillance of stock exchange members for insider trading. The New York Stock Exchange uses computer systems to monitor stock traffic for evidence of insider trading and to ferret out violators. The NYSE avoids directly piercing investor confidentiality by only accessing trading records once a market perturbation is otherwise detected, for instance, from volatile stock prices around the time of public disclosure of information material to the corporation's finances. Telephone Interview with Agnes Gautier, Vice President, New York Stock Exchange, Market Surveillance Division, March 28, 1995. For this reason, this market surveillance is not directly analogous to the monitoring of wire transfer traffic.

[90] Vicki Roberts, OTA Workshop, September 28, 1994.

[91] But the counterargument would run that industrial espionage is more easily achieved by using human contacts within corporations, that the huge amount of data comprising wire transfer traffic precludes unauthorized eyes from discerning anything interesting. Based on telephone interview with Donn Parker, SRI International.

**BOX 5-4: Telegraph and Early Wiretapping of Electronic Communications**

In the middle of the 19th century, the invention of the telegraph was soon followed by law enforcement and national security wiretapping, a vigorous policy debate over the sanctity of telegraphic communications, and legislative compromises modeled in part upon the protections extended to an analogous form of communication, the mails. Several similarities to the present issue bear mention for one. the telegraph network of the United States was in its infancy when the first wiretaps occurred. Moreover, the federal searches reached all telegraphs indiscriminately: no individual level of suspicion justified the search, as the telegraph companies were simply required to produce all outgoing telegram messages Later, state laws often distinguished between the clerk's copy of the outgoing or incoming telegram and the message in transit: the clerk's copies were given less protection than the communication in transit. And finally, just as banks argue today, telegraphic service providers pleaded the trust lodged in them by their customers, who expected confidentiality in telegraphic communications.

SOURCE David J Seipp, *The Right to Privacy in American History* (Cambridge, MA Harvard University, 1978).

greatly limits the capacity for abuse by competitors and others.

## ▮ Congressional and Judicial Solicitude for Corporate Confidentiality: Avoiding Economic Costs for Legitimate Participants in Funds Transfer Systems

The purposes of the following discussion of the common law and statutory protections for corporate confidential information are twofold: first, to underscore that corporations' subjective desire for confidentiality is recognized as reasonable, and second, to ask whether there are sufficient protections already on the books to guard against seepage of sensitive corporate information derived from wire transfer data beyond the authorized government use. In structure this problem is not new: in a wide variety of contexts confidential business information must be disclosed to the federal government.[92]

Congress has addressed this issue and legislated to protect confidential corporation information and communications. With the Trade Secrets Act, Congress criminalizcd a government official's unauthorized disclosure of confidential cororate information obtained in the coursc of thc regulatory relationship.[93] Moreover, this provision protects information beyond intellectual property and trade secrets to include a wide variety of business information, including profit and loss figures.[94] Also, the Freedom of Information Act (FOIA) exemption (b)(4) accords broad scope to the sort of confidential business information ("reverse FOIA") that cannot be released to parties requesting information pursuant to the Freedom of Information Act.[95] As further protection for

[92] Examples include the Federal Insecticide, Fungicide, and Rodenticide Act, codified at 7 U.S.C. 136h and the Toxic Substances Control Act, 15 U.S.C. 2613.

[93] 18 U.S.C. 1905.

[94] In the past, FedWire has demurred at supplying wire transfer records out of a fear of violating the Trade Secrets Act: the information in a wire transfer record has been construed as falling under the protections of the act.

[95] 5 U.S.C. 552(b)(4). Courts do not accept conclusory business arguments for sensitivity of information, however the business "has failed to show how analysis of the data. . would provide competitors with a profile of exactly how a defense contractor conducts its business.... [dis closure of the subcontracting amounts] reveals little of the factors involved in deriving those numbers. and therefore is unlikely to work a substantial harm on the competitive positions of defense contractors." *GC Micro Corp. v. Defense Logistics Agency* (9th Cir. August 26. 1994) (Docket No. 92- 15646)(rejecting the business claim that this data would provide competitors with a roadmap of the corporations" subcontracting plans and strategies).

sensitive information in the government's domain, Congress has made it a crime for a person knowingly to access information in federal computers without authorization or to access more information than authorized for that person.[96]

Alongside congressional recognition of corporate confidentiality, the courts have long recognized and protected sensitive commercial information. See, *Witkop & Holmes Co.* v. *Boyce*, 61 Misc. 126, 112 N.Y.S. 874 (1908):

> The names of the customers of a business concern whose trade and patronage have been secured by years of business effort and advertising, and the expenditure of time and money, constituting a part of the good will of a business which enterprise and foresight have built up, should be deemed just as sacred and entitled to the same protection as a secret of compounding some article of manufacture and commerce.[97]

Also, courts invoke "corporate privacy" routinely when limiting overbroad discovery requests in civil litigation. See, e.g., *GRET Corp.* v. *Shell Oil*, 138 F.R.D. 530 (1991).

*Tavoulareas* is noteworthy for its enunciation of a constitutional right of corporate privacy, limited as compared to the privacy rights of the individual[98] but more powerful than the public's First Amendment right to read published accounts of discovered material not used at trial. Significantly, both *Tavoulareas* and *Witkop* consider the value of customer names to the corporations a protected category of information and sought to protect against competitive harm.

## The Economic Costs of Surveillance of Legitimate Actors

Legislative and judicial protection of confidential corporate information both supports and undercuts a claim of confidentiality, however. On one hand, it signals that such information is respected by the federal government as privileged and dangerous if publicly distributed, and recognizes that the economic impact upon the violated business is grave enough to bring criminal penalties to bear against federal officials, who might otherwise be suborned by interested parties into releasing the sensitive information. On the other hand, the criminalization of the disclosure might allay the concerns of the corporation: with criminal sanctions in place for official misconduct, the question becomes what harm is there in having the government apprised of the details of wire transfers of law-abiding businesses?

In light of the fact that experts have suggested little ground other than utility for finding a right to corporate confidentiality, the debate about government access to wire transfer data would revolve around the feasibility and costs of minimizing the possibility of a damaging leak of

---

[96] 18 U.S.C. 1030(a). The several states have also sought to protected computerized information from unauthorized access. For example, the State of New York has criminalized a variety of computer intrusions, e.g. unauthorized use of a computer, computer trespass, computer tampering and the unlawful duplication of computer related material. New York Penal Law 156.05, .10, .20, .25, .26, .27 and .30.

[97] Quoted in *Tavoulareas* v. *The Washington Post Company*, 724 F.2d 1010 (D.C.Cir. 1984), *vacated* and *remanded*, 737 F.2d 1170 D.C. Cir. 1984).

[98] Even the natural person enjoys no constitutional right to informational privacy. *Paul* v. *Davis*, 424 U.S. 693 (1976)(holding that there was no constitutional basis for limits on disclosure of arrest records—they did not concern private conduct). But see *United States Department of Justice* v. *Reporters Committee for Freedom of the Press*, where the Supreme Court held that a clear privacy interest existed in a computerized compilation of an individual's criminal record. It appears that the computerized nature of the recordkeeping environment forced the Court to deviate from the *Paul* v. *Davis* precedent, a concern which recently rematerialized in *Arizona* v. *Evans*, *op. cit.*, footnote 48 (especially O'Connor's concurring opinion observing that "[w]ith the benefits of more efficient [computer-based recordkeeping systems] law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.").

information beyond the confines of the federal government.[99] That is, as the corporation cannot claim psychological damage from the unexpected disclosure of "private" thoughts or facts, the sole, but vital, basis for corporate grievance is economic: can a competitor's derivative use of the payments systems information impair the corporation's bottom line?[100] Can the government exert sufficient bureaucratic control over employees to prevent leakage and can security systems be installed to minimize the possibility of unauthorized access by employees and "crackers" alike?

The pertinent question becomes whether there are any models available for protecting information against unauthorized access. A recent OTA report, *Information Security and Privacy in Network Environments*, suggests that information security is rarely assured in the federal government, and in fact, many factors militate against guarantees of absolute security.[101] Nonetheless, the Census Bureau has a deep tradition of guarding against security breaches in its data and suggests a possible model. Currently, FinCEN utilizes access control and passwords, and has the potential for access monitoring to its Financial AI System (FAIS). But FinCEN does not use keystroke-monitoring to safeguard against unauthorized browsing in its FAIS, on the grounds that they trust their small cadre of five BSA analysts and that FinCEN lacks the computing capacity to install a monitoring apparatus atop the FAIS.[102] On the other hand, FinCEN keystroke monitors the Project Gateway access of state and local law enforcement, to deter and detect unauthorized access to CTR information. FinCEN also access monitors the more than one hundred authorized users of the IRS and Treasury Enforcement Communications System (TECS), both of which provide access to BSA data (see also chapter 3).[103] Experts within the banking community have opined that security systems in place at money center banks forestall bank employee abuse of the information contained in the wire transfer records, so it may be assumed that similar safeguards may be put in place at any central repository of wire transfer records.[104]

Recently a set of authors has proposed a solution for a similar problem of protecting sensitive business information in the very different context of permitting onsite inspections of chemical

---

[99] While this is a simple issue to formulate, the answer is elusive. The history of the Internal Revenue Service (IRS) is instructive in this regard: while more than twenty years ago the Nixon Administration abused confidential taxpayer information held by the IRS, lately, new, more mundane invasions of privacy have taken the form of numerous IRS employees browsing through taxpayer records, presumably at the behest of interested and paying parties. Other instances of government employees, such as Social Security Administration clerks, browsing through records to satisfy curiosity about celebrities, and their own acquaintances abound. See generally, Office of Technology Assessment, *Information Security and Privacy in Network Environments, op. cit.*, footnote 43, pp. 2-3, and 58 (setting forth instances of unauthorized browsing as well as some of the factors rendering ironclad security problematic).

[100] Perhaps a corporation could rely upon *Bellotti* and its confirmation of the corporation's right to speak politically for the argument that premature disclosure of political thoughts would prejudice a corporation's right to deliberate and speak politically, however, given the very limited and almost utterly nonpolitical nature of wire transfer information, this argument would stretch credulity.

[101] The General Accounting Office (GAO) has identified employee browsing through the National Crime Information Center as well as the IRS: employees have browsed records relating to friends, family, neighbors and celebrities. Office of Technology Assessment, *Information Security and Privacy in Network Environments, op. cit.*, footnote 43, pp. 2-3.

[102] Interview with Ted Senator, Chief, Artificial Intelligence Division, FinCEN, August 25, 1994.

[103] The GAO noted that more than 270,000 queries of the BSA database and 66,000 separate sessions took place in an eighteen month period ending June 30, 1993. This volume of queries would be a challenge to keystroke monitoring. U.S. Congress, General Accounting Office, *Money Laundering: Progress Report on Treasury's Financial Crimes Enforcement Network*, (U.S. Government Printing Office: Washington, DC November 1993).

[104] But it is unlikely that financial institutions would fully disclose security breaches lest their customers seek out financial institutions with better information security.

weapons production facilities to verify compliance with the Chemical Weapons Convention.[105] Chemical weapons manufacturers fear that international inspectors will reveal trade secrets and other proprietary business information following comprehensive onsite inspections and data collection from chemical weapons manufacturers.[106] The Chemical Weapons Convention contains a variety of familiar provisions to control data leakage, including requirements for secure storage, coded identification of manufacturing facilities, as well as nondisclosure agreements. Nonetheless, the United States may not sign the treaty, due in part to industry concerns about loss of confidential business information. Among other proposals for assuaging industry concerns, Tanzman et al. propose alternative remedies beyond those of the Trade Secrets Act. It is proposed to allow the Tucker Act to confer jurisdiction to sue the United States for compensation for the loss of confidential business information.[107] Independent of the precise limits of "takings" analysis suggested by *Ruckelshaus* v. *Monsanto*[108] (and whether, in fact, a "taking" could occur in the context of wire transfer reporting), Congress could specify a statutory compensation regime for economic harm resulting from unauthorized access to wire transfer information within the government's control. In order to minimize litigation costs, standards for evidence could be specified (e.g., use of access logs and keystroke-monitoring logs as self-authenticating evidence) and alternative dispute resolution processes could be used to speed redress and minimize litigation costs.[109] This might diminish the problems of causality—the link between the government holding of the wire transfer records and the economic harm—an especially crucial concern where other parties are privy to the wire transfer data, including originating, beneficiary and intermediary banks, as well as the originator and beneficiaries themselves. Nevertheless, the waiver of sovereign immunity, or consent to be sued for loss of confidential business information, would impose a salutary incentive on agencies in possession of the confidential wire transfer records, particularly if any damages claims were required to come out of the agencies' general appropriations.

## CONCLUSIONS

This chapter has set forth many of the concerns that would plague the indiscriminate monitoring of wire transfer traffic. More finely detailed assessment of the costs of the various technological configurations as well as necessary statutory changes are spelled out in Chapter 7. As a general matter, however, facilitating the technological configurations would further underscore the unsettled and "patchwork" nature of "data protection" in the United States, requiring a roll-back in existing privacy protections. A further complica-

---

[105] Barry Kellman, David S. Gualtieri and Edward A. Tanzman, "Disarmament and Disclosure: How Arms Control Verification Can Proceed Without Threatening Confidential Business Information," 36 *Harvard J. Intl. Law* 71-126 (Winter 1995), citing the *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, opened for signature* January 13, 1993, 32 *I.L.M.* 800 (not in force).

[106] *Ibid*. at 74.

[107] The Tucker Act is codified at 28 U.S.C. 1491(a)(1).

[108] 467 U.S. 986 (1984). *Monsanto* is noteworthy in several respects. First, intangible proprietary information is recognized as "property" protected by the Fifth Amendment. Furthermore, the Court observed that government could "take" property, prompting a claim for just compensation, even if government did not acquire or destroy the property. A mere interference with reasonable investment-backed expectations can cause a "taking" under the Fifth Amendment. In the wire transfer context, the argument remains to be made that the mere reporting of wire transfers would interfere with investment-backed expectations. In *Monsanto*, the Court considered the legislatively mandated sharing and sale of proprietary data to competitors to be possible "takings."

[109] Cf. Tanzman *et al., op cit.*, footnote 105, pp. 122-124. This proposal would raise budgetary issues—at what weight would this contingent liability be assessed by the Congressional Budget Office?

tion stems from the fact that European countries are moving toward a uniform regime protecting data against secondary use not consistent with the purpose for which it was collected.[110] Any monitoring proposal runs contrary to this fundamental precept of European data protection and fair information practices.

As noted in the preceding discussion, however, there is a long tradition of assessing "privacy" concerns from the perspective of the Fourth Amendment and the Constitution in this country, a tradition that might suggest that the overlaying of fair information practices or "data protection" is unnecessary or inapposite for deciding questions of law enforcement access to information. Several arguments drawn from American legal thought undercut the claim that wire transfers might have for freedom from law enforcement access. Transactions within the stream of commerce receive diminished protection under the Bill of Rights. Moreover, the kind of information in a wire transfer is at a considerable remove from the core concerns of the Fourth Amendment, political thought and the sanctity of the home.

Yet, confidentiality in business communications still looms as a large concern, although this concern may be partly addressed by ensuring proper security safeguards for the wire transfer data. An extreme measure to protect the data would be a waiver of sovereign immunity, to permit corporations to sue the government for economic damages suffered. This would require Congress to pay for the privilege of endangering corporate confidential business information, impose incentives on the handlers of data to safeguard it, and hence preserve the corporation's incentive to engage in entrepreneurial conduct.

[110] The European treaties and laws on data protection, including the recently adopted European Union Data Protection Directive, are discussed at greater length in the following chapter.

# International Issues 6

Law enforcement efforts focusing only on domestic wire transfers would be of little utility, in view of the transnational nature of much money laundering.[1] Moreover, a screening system's best chance of success may be with international wires, where there are additional markers of suspiciousness, such as country of origin or receipt,[2] route through an offshore banking haven, or connection to an anomalous non-export related business.

As noted in previous chapters, the incoming wire transfer has become increasingly interesting to law enforcement, with the growing realization that money launderers find the United States a stable and attractive site for investment, particularly in comparison with countries undergoing political risk and currency upheavals.[3] But access to international wire transfers raises policy questions beyond those of monitoring domestic transfers. While U.S. law enforcement may currently subpoena international wire



[1] For instance, the American Express Bank International of Texas laundered funds through the Cayman Islands, ultimately paying a $32 million fine. New York *Times*, Nov. 22, 1994, p. A1(N), p. D2.

[2] Not every international wire transfer will be transparently international: a U.S. bank with foreign subsidiaries may number foreign accounts differently, thus what appears to be a domestic transfer to the U.S. bank may suffice to transfer funds to an account held by the foreign subsidiary.

[3] At the same time, there are substantial questions about the difficulty of detecting incoming money laundering wires in light of the fact that the money has already been laundered to the point where its owner is confident about returning or bringing the funds to the United States. Others believe that the domestic legs of an international funds transfer may themselves raise suspicions, as was observed in the Bank of Commerce and Credit International (BCCI) case, characterized by a churning of money through transfer after transfer.

transfer records held by U.S. banks,[4] information regarding the originator of the wire transfer may have already been lopped off or protected by the originating foreign bank. Foreign bank secrecy laws, which entail the possibility of criminal sanctions being brought against foreign banking officials responsible for revealing financial information about their customers, may be a significant impediment to tracing the flow of funds back to their source, as is the profit incentive informing bank secrecy laws in the first place.

The role of offshore banking havens in the legitimate and illegitimate economies of the United States and the world is discussed in this chapter. Offshort banking havens present a twofold problem for wire transfer screening systems. First, they undermine the utility of monitoring incoming wire transfers by the financial anonymity they can provide. Second, they compete with U.S.-based banks, undercutting the acceptability of monitoring to the banking community in the United States, particularly as monitoring may threaten the lucrative dominance of the dollar in international payment systems. The more scrutiny directed at customers of U.S. financial institutions, the more attractive offshore banking havens will become.

This chapter will also discuss data protection initiatives governing the transborder flow of information, generated by the European Union (EU), the Council of Europe, and the Organization for Economic Cooperation and Development (OECD). The unilateral monitoring of international wire transfers could damage international relations, particularly with close allies in Europe.[5] It could even imperil otherwise fruitful cooperation in the pursuit of money laundering among international law enforcement bodies.[6]

Finally, this chapter will look at the efforts of the United States in combating international money laundering, unilaterally and through multilateral and bilateral cooperation and agreements aimed at criminalizing money laundering, creating cash transaction records and gaining cooperation in the piercing of bank secrecy. The issue of access to international data becomes embroiled in the conflict between expanding notions of sovereignty and the effects of communications networks. One solution to this tension might be multilateral negotiations aimed at the control of money laundering by permitting law enforcement access while otherwise preserving a state's legitimate interest in bank secrecy and data protection. Bank haven countries, however, might be expected to resist such efforts.

## ACCESS TO INTERNATIONAL WIRE TRANSFER INFORMATION

### Foreign Bank Secrecy

Foreign bank secrecy laws do not curtail the ability of U.S. law enforcement to subpoena international wire transfer records held domestically (see box 6-1). Nevertheless, these laws and the ethos underlying them do present a potential impediment to obtaining comprehensive information on international wire transfer and following up on investigative leads. In general, bank secrecy laws prohibit banking officials from releasing confidential customer information to third parties outside the financial institution. Bank secrecy may be

[4] Under section 1515 of the Annunzio-Wylie Anti-Money Laundering Act of 1992, Treasury and the Federal Reserve Board may "request" from U.S. banks international funds transfer records required to be held by the wire transfer regulations. 12 U.S.C. 1829b(b)(3)(C). As the regulations only take effect on the first of January 1996, this "request" authority has not yet been tested.

[5] This conflict will become sharper with the promulgation of the final version of the European Union's (EU) Data Protection Directive (see text *infra*).

[6] Access to international wire transfers for U.S. law enforcement raises the question of whether the United States should risk interfering with the international flow of capital, with the unlikely but potentially dire effects of discouraging foreign direct investment in the United States. In addition, the United States has security interests in the use of the dollar-based payment system, since economic sanctions depend on blocking/freezing of assets held by or going through U.S. banks.

## BOX 6-1: Nonspecific Subpoenas Targeting International Wire Transfers

Comity or the voluntary deference of U.S. courts to foreign laws (for example, bank secrecy laws), complicates efforts at reaching records held offshore In the 1980s, the U.S. Internal Revenue Service (IRS) served a "John Doe" or nonspecific, subpoena on several northern California banks, seeking records related to international funds transfers to certain tax haven countries Although the Bank of America had cooperated and produced copies of wire transfer records held in the United States involving wire transfers to and from certain countries, in the early 1990s, the IRS sought to enforce the subpoena and obtain records relating to wire transfers held by a Bank of America subsidiary in Hong Kong. Hong Kong has a general commercial confidentiality statute, Protection of Trading Interests Act of 1980, criminalizing the disclosure of commercial Information. A federal district court refused to require that Bank of America produce the records held abroad. *In re the Matter of Tax Liabilities :John Does, No C-88-0137* Misc (N D Cal., March 11, 1992) (Wieking, J.) The district court applied section 442 of the American Law Institute's *Restatement of the Law (Third) on the Foreign Relations of the United* States,[1] in finding that the subpoena was "generic in its terms and in its purpose [not] aris[ing] from an Investigation of any particular alleged misconduct, nor does it seek evidence of particular Identified transactions. " *Ibid.,* p. 15. Under section 442, these factors cut against enforcing the subpoena with respect to records held abroad, even though the vital U.S. interest in detecting tax evasion was implicated The district court's ruling is the flip side of holding U.S. subsidiaries of foreign banks to the U.S. standard in producing records held in the United States, by the same token, U S banks doing business abroad will take on characteristics of the bank secrecy jurisdiction hosting them.

A salient point is confirmed by this case: apparently the Protection of Trading Interests Act did not bar the transmission of the wire transfers to the United States even though authorities in Hong Kong were on notice that the records would be scrutinized by U.S. government authorities That aspect of the John Doe, or nonspecific, subpoena was upheld in Northern California, and had resulted in the disclosure of some 13,000 wire transfer records to the IRS as of March 1992, leading to 10 cases referred for criminal prosecution

[1]Section 442 of the Restatement states that a court or agency should only issue a subpoena or summons upon consideration of the importance of the information sought, the degree of specificity of the request, the provenance of the information in the United States or abroad), the availability of alternate means of gaming the Information, the extent to which compliance with the summons would trench on the foreign nation's interest and the extent to which noncompliance would adversely affect U S interests

SOURCE Off Ice of Technology Assessment, 1995

a matter of common law, civil or penal law, or perhaps even a constitutional precept.[7] There are two kinds of bank secrecy laws—"blocking statutes" and true bank secrecy provisions such as Article 47 of the Swiss Confederation. The latter involve the legal requirement of confidentiality of information and impose civil or criminal penalties for unauthorized disclosure of customer informa-

[7]Article 18 of the Spanish constitution guarantees secrecy of communication and limits the use of personal information in order to protect personal privacy. This article would likely shelter financial data.

tion.[8] In the Bahamas, bank secrecy provisions penalize improper disclosure with the possibility of a two-year prison sentence.[9] Blocking statutes, on the other hand, do not establish a confidential relationship between customer and bank. They are invoked only when a foreign law enforcement agency attempts to access account records, may be waived only by the sovereign, and represent the efforts of states to resist extraterritorial application of another state's laws.[10]

Foreign bank secrecy and blocking laws affect investigations in the United States primarily through the judicial doctrine of "comity," or a U.S. court's "essentially voluntary deference to the acts of other governments, undertaken for the common good even though no transnational institution exists to exert any compulsion."[11] This doctrine usually arises when U.S. law enforcement seeks to enforce a subpoena directed at records held abroad in a bank secrecy jurisdiction. The basis for comity is the perception that a state should forbear from presenting the citizen of another sovereign with the alternative of violating either its laws (i.e., by refusing to obey a court order to present records) or the laws of the citizen's sovereign, specifically, foreign bank secrecy laws prohibiting the disclosure of bank records. But some U.S. courts have found that the national interests in stemming illegal drug trade are more vital than any foreign interest in bank secrecy (a factor in the balancing test of whether to impose contempt on a non-complying bank officer).[12] Other courts have been even less solicitous of comity concerns, finding merely that a willingness to do business in the United States fairly subjects a corporation to the relative rigor of U.S. criminal investigations.[13]

Again, bank secrecy is not necessarily an absolute barrier to law enforcement, particularly once an investigation has yielded strong evidence about criminal conduct of accountholders in bank secrecy jurisdictions. Bank secrecy jurisdictions have come to recognize that their laws may shelter narcotics traffickers and have begun cooperating with international law enforcement efforts. Switzer-

---

[8] The Swiss Federal Law on Banks and Savings Banks, article 47 provides in part:

Persons who disclose confidential information entrusted to them or which has come to their knowledge in their capacity as official, [or] employees [of banks]. . . shall be penalized by imprisonment not to exceed six months or a fine not to exceed SFr. 50,000.

Reprinted and translated in *Federal Law on Banks and Savings Banks* (Switzerland: Union Bank of Switzerland, 1990).

It is highly interesting to observe that in Swiss criminal cases, bankers may be obliged to testify and produce relevant documents, as reflected by clause 4 of Article 47—"Federal and cantonal regulations regarding the obligation to testify and to furnish information to government authorities shall also apply." *See also* Dunant, Olivier and Wassmer, Michele, "Swiss Bank Secrecy: Its Limits Under Swiss and International Laws," 20 *Case W. Res. J. Int'l L.* 541-575, pp. 549-550 (1988).

[9] Banks and Trust Companies Regulation Act of 1965, 1965 Bah. Acts No. 64, art 10, *as amended by* Banks and Trusts Companies Regulation (Amendment) Act, 1980, 1980 Bah. Acts No. 3.

[10] Many blocking statutes, designed to thwart foreign governments' access to records, were enacted in direct response to U.S. extraterritorial subpoenas. The Restatement of the Law of Foreign Relations of the United States (Third), at 442, note 4 (1987). As of 1986, some fifteen states had adopted legislation expressly designed to counter United States efforts to secure production of documents located outside the United States. *Id.* at 442, Reporters' Note 1. These countries include the United Kingdom and France.

Section 442 provides guidance to U.S. courts in their enforcing of subpoenas with international dimensions. Significantly, section 442(c) directs the court to take into account "the degree of specificity of the request" and "whether the information originated in the United States."

[11] 18 Wright, Miller & Cooper, *Federal Practice and Procedure*, 4473 (1981).

[12] *United States* v. *Bank of Nova Scotia (II)*, 740 F.2d 817, 827 (11th Cir. 1984), *cert. den'd*, 462 U.S. 1119 (1985); *United States* v. *First National Bank of Chicago*, 699 F.2d 341, 347 (7th Cir. 1983) (nonetheless overturning a district court's contempt order sanctioning defendant for failing to comply with a subpoena for records of alleged tax evaders).

[13] See, e.g., *In re Grand Jury Proceedings United States* v. *Field*, 532 F.2d 404, 410 (5th Cir.), *cert. den'd*, 429 U.S. 940 (1976).

land, for example, has signed a Mutual Legal Assistance Treaty (MLAT) with the United States,[14] ended anonymously held bank accounts and now requires the beneficial owner's name to appear on bank records.[15]

Even if the letter of bank secrecy laws does not impede the monitoring of international wire transfers, the ethos of confidentiality for a price works against the success of any monitoring proposal. Bank secrecy is lucrative both for the banks and their host countries. Hence, foreign bankers might be expected to strip away the history of a wire transfer before its ultimate transfer into the United States. These precursor wire transfers, while not necessary for completing the transfer and perhaps impossible to fit into existing wire transfer formats, are most interesting to U.S. law enforcement. Even if the United States were to refuse to permit domestic banks to process incoming wires that did not have names in the originator fields (as the U.S. Treasury Department's proposed 1989 wire transfer rules provided[16]), a bank could still please both sovereigns by inserting plausible yet false names in the originator field; accurate originator information is not necessary to the successful processing of the transaction.[17]

## The Role of the International Offshore Bank in the World Economy

With the dramatic rise of international banking havens over the past 30 years, obscure island nations have surged to prominence in the international banking economy.[18] Legitimate businesses have long banked in and routed wire transfers through secrecy jurisdictions.[19] Banks book assets on behalf of their customers in offshore banking havens in part to avoid Federal Reserve requirements: slightly higher interest rates may be paid on customer funds held offshore, since the bank need not hold the reserve amount in a non-interest-bearing account with its district Federal Reserve Bank. Early newspaper accounts indicate that Barings Bank opened a special account in the Cayman Islands to cover margin calls for the futures trading of Nicholas Leeson, perhaps to skirt Bank of England regulations requiring notice when more than

---

[14] The U.S.-Switzerland Mutual Legal Assistance Treaty was successfully invoked as early as 1978, in the prosecution of Stanley Mark Rifkin, who fraudulently wire transferred money from a Los Angeles bank account to his Swiss bank account. James I.K. Napp, "Mutual Legal Assistance Treaties as a Way to Pierce Bank Secrecy," 20 *Case Western J. Int'l Law* 405-433, 405 (1988).

[15] Switzerland is a member of the Financial Action Task Force (to be described below) and has agreed on to the Forty Recommendations of FATF, including the prohibition on anonymous transactions.

[16] *Bank Secrecy Act Regulatory Applications to the Problem of Money Laundering Through International Payments*, 54 *Fed. Reg.* 45769, 45771 (Oct. 31, 1989)(requiring that all international wire transfers contain all known originator and beneficiary identifying information).

[17] One commentator cites several wire transfer experts stating that nonsense words could fill any mandatory "on-whose-behalf" field. Sarah Jane Hughes, "Policing Money Laundering Through Funds Transfers: A Critique of Regulation Under the Bank Secrecy Act," 67 *Indiana Law J.* (Winter 1992), 283-330, 296, n.77 and 305 (citations omitted).

[18] Vanuatu (in the South Pacific), Niau, Republic of Nauru, and St. Kitts, *inter alia*. See chapter 4, footnote 31 for a complete list. Long ago, Congress recognized the role that banking haven countries played in abetting tax evasion and other crimes. The 1970 Bank Secrecy Act requires that U.S. nationals file yearly Foreign Bank Account Reports with the Internal Revenue Service (IRS) detailing foreign accounts and transactions with foreign banks in excess of $5,000.

[19] Susan Roberts, "Fictitious Capital, Fictitious Spaces: the Geography of Offshore Financial Flows," in Stuart Carbridge, Nigel Thrift and Ron Martin (eds.), *Money, Power and Space* (Oxford, U.K.: Blackwell, 1994), pp. 91-115.

25 percent of a group's capital is transferred to a subsidiary.[20]

A former investigative counsel with the Senate Foreign Relations Committee, Jack Blum, notes that judging by its wire transfer traffic, the Cayman Islands represent the fifth largest banking economy in the world.[21] Blum and others have explored the role of offshore banking havens, arguing that the bank secrecy offered by these jurisdictions attracts either those seeking to avoid regulation and taxation or those whose source of funds is itself illicit, such as the narcotics trafficker.[22] Professor Ingo Walter observes that banking offshore carries dramatic costs, such as political and country risk, and increased risk of loss by embezzlement or failure of loosely regulated and uninsured banks.[23] That offshore banking havens thrive underscores the paramount value of secrecy to the haven's clientele. In addition to the advantages of maintaining anonymous accounts (or accounts held in fictitious names), banking havens frequently offer for trivial amounts of money the protective mask of anonymous and bearer corporations.[24] The bearer corporation further complicates law enforcement's mission: even if bank secrecy is pierced, law enforcement may be no nearer to discovering the beneficial owner of the funds.

Offshore banking havens have thrived partially in response to U.S. regulatory requirements and a lack of bank secrecy in the United States. A further escalation in scrutiny by law enforcement or banking regulators may have the effect of increasing the tendency to place assets abroad in secrecy jurisdictions, eroding profit centers for U.S. banks and ironically increasing the difficulty of conducting criminal investigations.[25] A wire transfer monitoring system could further heighten the competitive disadvantage of U.S. banks vis-à-vis banks in loosely regulated bank secrecy jurisdictions. This competitive disadvantage would be exacerbated by the imposition of further compliance costs on banks and by creating too large a gap between the United States and the rest of the world in terms of policing money laundering.[26]

Offshore banking havens raise a related question: would monitoring deter foreign nationals and corporations from routing their wire transfers through New York? Concerns about undermining

---

[20] *Washington Post*, March 6, 1995, p. A13.

[21] The islands are also the sixth largest source of bank loans to the United States from abroad. *Recent Developments in Transnational Crime Affecting U.S. Law Enforcement and Foreign Policy,* Hearing before the Subcommittee on Terrorism, Narcotics and International Relations of the Committee on Foreign Relations, United States Senate. S. Hrg 103-606, p. 136. Senator Kerry stated that the Cayman Islands hold some $400 billion in assets, with a population of only 26,000. *Ibid.*, p. 4.

[22] Even well-known banking havens, such as Panama under Noriega, have had legal mechanisms for piercing secrecy, such as Law 23 of December 31, 1986, permitting Panamanian officials to provide information when requested by foreign authorities. Statement of Assistant Attorney General Jo Ann Harris, S. Hrg. 103-606, p. 38.

[23] Ingo Walter, *The Secret Money Market: Inside the Dark World of Tax Evasion, Financial Fraud, Insider Trading, Money Laundering, and Capital Flight* (New York, NY: Harper & Row, 1990), p. 7.

[24] A fully anonymous shell corporation may be bought in Turks and Caicos Islands for as little as $10,000, a trivial sum in relation to the sums of money that may be laundered through it. A bearer corporation is owned by whoever holds the corporation's shares (i.e., the shares are not listed to a particular owner). Furthermore, no public records are kept as to the holder of the shares, and transfer of the corporation (and its assets) may be effected informally, by the handing off of the paper documents. Jack Blum, CSIS Conference on Global Organized Crime, September 26, 1994. Blum also noted that the relatively insignificant costs of buying anonymity would defeat any attempts to detect patterns of wires involving certain entities, so long as the launderer were willing to discard anonymous corporations after several uses.

[25] Recent U.S. efforts to control transfer pricing abuse and offshore trusts may strengthen the incentive of some to find alternative mechanisms for moving money, so as to avoid U.S. regulation and intrusions into secret movements of money.

[26] Extreme solutions to the problem posed by offshore banking havens have been proposed: in fact, the Kerry Amendment, section 4702 of the Anti-Drug Abuse Act of 1988, requires the President to bar from U.S. dollar clearing or wire transfer systems known money launderers, as well as countries and banks facilitating money laundering. 31 U.S.C. 5311, note. This provision has never been invoked.

the preeminence of the U.S. dollar as the medium for international transactions may be exaggerated, however. The financial solidity and history of gross netting of real-time payments in New York militate against mass defections to other wire transfer systems worldwide. CHIPS is the premier international payment system, and CHIPS's appeal is, and would remain, the extensive correspondent relationships of its member banks, who may then offer lower cost book transfers to complete wire transfers.

But some commentators emphasize that only historical accident has led to many international transactions relying upon the dollar as the conversion currency between two foreign currencies.[27] It is possible that, on the margins, transferors particularly valuing confidentiality might take a chance on new gross settlement wire transfer systems, particularly the one proposed by the Bank of Japan, which would also have the advantage of involvement of a central bank, a stable currency, and a stable political climate. Over time, confidence in new systems could be gained and true competition might ensue, to the detriment of U.S. payment systems with compromised confidentiality.

## European and Other Data Protection Initiatives

An additional impediment to the proposed monitoring derives from European data protection initiatives governing the uses of electronically stored data and its transborder flow. These initiatives all aim to protect data generated within a country's borders, even as the data crosses international borders. Generally, information may be prohibited from leaving a signatory country if it means entering a country with less stringent data protection laws.[28] Several international bodies have already addressed the issue of electronic data protection (U.S. experts usually term this "information privacy"), with the OECD Guidelines and the Council of Europe's Convention issued more than a decade ago. For instance, on July 25, 1995, the Council of Ministers of the European Union adopted the Directive on Protection of Personal Data (the EU Data Protection Directive).[29] All of these data protection initiatives must be implemented into national law through the regular legislative channels of a signatory country before they have binding effect.

---

[27] See, e.g., Hughes, "Policing Money Laundering Through Funds Transfers," *op. cit.*, footnote 14, pp. 312-313 (citations omitted). Hughes argues that offshore netting is a distinct possibility due to enhanced recordkeeping (*not* reporting) requirements proposed by Treasury in 1990.

[28] Professor Joel Reidenberg notes several instances where, pursuant to domestic law, foreign governments have "prohibited the transmission of personal information to countries perceived as ignoring computer privacy concerns," including the French and British governments prohibiting data transfers to the United States. Joel Reidenberg, "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" 44 *Federal Communications Law Journal* 195-243, 199 & n. 16 (March 1992). David H. Flaherty, the Data Protection Registrar for the Canadian province of British Columbia, cautions that European data protectors "anticipate blocking the movement of personal data from European branches of multinationals to Canadian or American branches, because equivalent data protection does not exist." *Telecommunications Privacy: A Report to the Canadian Radio-Television and Telecommunications Commission*, 73 (1992). Currently, the Electronic Communications Privacy Act (ECPA) would sufficiently protect wire transfer data to satisfy the European and OECD initiatives. OTA is aware of no instances where international wire transfers to the United States have been barred by foreign data protection standards or commissioners.

[29] Citations to the Directive are to the "Common Position" approved February 20, 1995. Some view protection of transborder flows of information to be subtle non-tariff barriers to trade. See, e.g., the Business Roundtable Statement on Transborder Data Flow: "International Information Flow: A Plan for Action," *reprinted in* L. Richard Fischer, *The Law of Financial Privacy: A Compliance Guide* (2nd edition)(Warren, Gorham & Lamont: Boston, 1991) 6-89 to 6-125, A6.3. Others regard the EU Data Protection Directive as a "threat [to] U.S. leadership in the information economy" by its restrictions on transborder flows to the United States. Fred H. Cate, "The EU Data Protection Directive, Information Privacy and the Public Interest," forthcoming in 80 *Iowa L. Rev.*, (April 1995).

While similar in topic and scope of protection, there are substantial differences in legal effects of the various data protection initiatives and national data protection laws. At least 15 states have enacted data protection laws, including Australia, Austria, Belgium, Denmark, France, Germany, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. Others are on the brink of doing so: Finland, Iceland, and Italy.[30] While national law is ultimately what shapes data protection policies, for purposes of economy, this chapter will focus on the initiatives themselves.

In 1980, the OECD[31] issued its *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Guidelines").[32] The OECD Guidelines seek voluntary compliance by signatory states.[33] They recommend limits on the collection of data, a relevancy requirement, a 'purpose' limitation on the use of data, reasonable security safeguards, and prohibitions on disclosure without the subject's consent or authorization. Part 3 of the OECD Guidelines provides that a member country should permit the export of data to another member country, provided that the receiving country observes the guidelines' principles.

The *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* ("European Convention")[34] was concluded within the framework of the Council of Europe.[35] The European Convention is an international treaty and requires signatory states to incorporate its principles into their domestic law by normal parliamentary procedures. Until this is done, the treaty grants no rights directly to individuals within a signatory state. This "executory" status of the European Convention, as well as the EU Data Protection Directive, is significant for it underscores that national law is paramount and thus individual signatory states may treat U.S. practices regarding international wire transfers differently.[36]

Also under the aegis of the Council of Europe, the Council of Ministers has set forth sectoral recommendations for the access and dissemination of specific types of data. These solely advisory recommendations are addressed to the governments of the member states, "inviting them to take account of the solutions offered in the recommen-

---

[30] Fischer, *ibid.*, 6-9 to 6-10, ¶6.04.

[31] The Organization for Economic Corporation and Development (OECD) consists of the states of Western Europe, North America, New Zealand, and Japan. The OECD guidelines have been adopted in one form or another by 24 countries (e.g., the United States, Australia, Canada and New Zealand do not protect data handled by private corporations). Nations adopting the guidelines consist of Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. A. Neisingh, A. and J. de Houver, translated as *Transborder Data Flows* (New York, NY: KPMG, 1988), p. 27.

[32] O.E.C.D. Doc. No. C(80)58 (Final) (September 23, 1980), *reprinted in* 20 *I.L.M.* 422-427 (March 1981).

[33] Reidenberg, "Privacy in the Information Economy," op. cit., footnote 28, n. 21.

[34] Euro. T.S. No. 108 (Jan. 28, 1981) ("European Convention"), *reprinted in* 20 *I.L.M.* 317-325 (March 1981). This convention entered into force by late 1987 and until recently was the only binding international instrument on data protection.

[35] The Council of Europe consists of Andorra, Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, San Marino, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, and the United Kingdom. The Convention has entered into force in Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Ireland, Luxembourg, the Netherlands, Norway, Portugal, Slovenia, Spain, Sweden, and the United Kingdom.

[36] Actually, Title VI of the French Constitution, in certain circumstances, may incorporate automatically international treaties, including EU Directives, directly into French national law.

dations when they are dealing with the particular data protection issues discussed in the recommendations."[37] These recommendations include *Protection of Personal Data Used for Payment and Other Related Operations* ("the Council of Europe's Recommendation")[38].

The European Union's *Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data and on the Free Movement of Such Data* has only recently been formally adopted.[39] It is expected that it will include a provision requiring the member country's data protection commissioner to prohibit exports of "personal data" when the receiving country does not possess adequate data protection laws.[40]

The EU Data Protection Directive applies only to "personal data," defined as any information relating to an identified or identifiable *natural* person.[41] Generally, personal data may be processed only with the consent of the data subject. The data subject usually must be provided with certain mandatory disclosures if data is to be collected, processed and/or distributed to a third party. He or she must also have access to the data; the opportunity to object to its collection, processing and/or disclosure; and the opportunity to correct any factual errors.

### *Unresolved Questions From the Data Protection Initiatives*

An initial problem in exploring the implications of these data protection initiatives stems from the term "personal data." The European Convention defines "personal data" to include any information relating to an identified or identifiable person (the "data subject").[42] National legislation implementing the European Convention generally has not extended the term "personal data" to include corporate data.[43] The Council of Europe's Recommendation notes this phenomenon, advising further that countries are free not to protect legal persons, although the Recommendation expresses solicitude for the closely held corporation, insofar as its records begin to reflect personal information.[44]

A second unresolved question is the scope of the Recommendation, the most detailed instrument regarding financial data protection. Its drafters frequently note that they intend to give the term "means of payment" as broad a reading as possible. The Explanatory Memorandum to the Recommendation underscores that the recommendation addresses at least consumer electronic payment systems, such as smartcards and electronic funds-transfer/point-of-sale transactions

---

[37] Explanatory Memorandum to Recommendation No. R(90)19, paragraph 2 (Council of Europe, 1992).

[38] Recommendation No. R (90)19 (Council of Europe, 1992).

[39] Originally issued at 1990 O.J. (C277), Com(90)314 Final SYNS 287 (Sept. 13, 1990). The Common Position of the Council of Ministers is found at 1995 OJ (C 93) (13 April 1995). Citations to the EU Data Protection are to the Common Position.

[40] Article 25(1) specifies that "Member States shall provide that the transfer to a third country of personal data. . . may take place only if. . . the third country in question ensures an adequate level of protection." American corporations "fear that they will be unable to move. . . data legally—even if they own it—to the United States." Fred H. Cate, "Protecting Information Privacy," *The Annenberg Washington Program Update,* vol. 2 no. 2 (November 1994), p. 4.

[41] Article 2(a).

[42] Article 2 subdivision a.

[43] Norway, Austria, Denmark and Luxembourg protect the records of corporations and legal persons. Fischer, 6-9, ¶ 6.04, fns. 56-58. By way of contrast, the UK Data Protection Act 1984 protects only identifiable, living persons.

[44] Op. cit., footnote 38, ¶ 31.

(EFT-POS). The references and examples of "means of payment" are consistently consumer systems: EFT-POS, automated teller machines (ATM), credit card, and, prospectively, smart card and digital money.[45] This suggests that wholesale wire transfers do not fall within the ambit of the Recommendation. The strongest evidence that the Recommendation would apply to wholesale wire transfer systems comes in an aside in paragraph 36 of the appendix: SWIFT is referenced, in excluding from the Recommendation's scope the telecommunication operator which leases a line to the "communication network operator," or SWIFT. Implicitly, it would appear that SWIFT's messages, including instructions to execute book transfers, are within the scope of the Recommendation. Nevertheless, the Recommendation is solely hortatory, and it remains to be seen whether individual states choose to bring wholesale wire transfers under their data protection regimes.

A third issue looms in the question of extraterritoriality. Could a European country draft legislation that would punish an action of a U.S.-domiciled bank or wire transfer system? Or might a signatory state hold its own banks vicariously liable for monitoring taking place in the United States? This question would arise where the European bank *must* disclose the data in order to execute the customer's wire transfer instructions. Countries with data protection laws may punish banks, both criminally and civilly, for actions of unrelated parties in foreign states.[46] The Recommendation itself sanctions the use of data in order to complete a transaction, raising the possibility that the disclosure of wire transfer data to a U.S. recipient bank would comply with the dictates of say, the German law, which holds that "personal data may be disclosed to third parties only if the disclosure serves the purpose of a contractual or [other] obligation."[47] This argument, that the disclosure is implicitly permitted, is partially undercut by the fact that the originator need not be identified by the originating bank for the transaction to be executed, hence the originator's consent

[45] For example, paragraphs 4 and 5 of The Explanatory Memorandum to the Recommendation underscore that the document addresses consumer electronic payment systems, such as smartcards and electronic- wire-transfer/point-of-sale (EFT-POS) transactions.

[46] Joel Reidenberg suggests in an upcoming article in the Iowa Law Review that countries may hold their banks strictly liable for secondary use processing in other countries, or countries may simply block the export of data if secondary use systems are in place. forthcoming in 80 *Iowa L. Rev.*, (April 1995). One example is the recent Quebec data protection law, chapter 17, *Loi sur la protection des renseignements personnels dans le secteur privé*, (adopted June 15, 1993). Any of the technological configurations set forth in chapter 7 would raise this secondary use issue, whether a U.S. bank or U.S. law enforcement was conducting the secondary use. Some U.S. banks already scan all wire transfers in seeking to comply with Office of Foreign Assets Control (OFAC) prohibitions on financial transactions with certain blocked countries and designated banks and individuals. (See discussion of the OFAC system in chapter 4).

Also, the U.K. Data Protection Act 1984 requires that data collectors register with the British government and specify potential countries that might receive data. The Act sets out civil and, potentially, criminal sanctions for violations. See World Wide Web site: http://www.open.gov.uk/dpr/dprhome.htm (May 9, 1995).

[47] The EU Data Protection Directive also speaks to the issue of transborder flow of "personal data" and may prohibit it even where the export and potential disclosure is essential to the customer's intent. One expert opines that express customer consent may not suffice to waive the proscription against the export of data to a country with inadequate data protection standards. Telephone interview, Professor Fred H. Cate, Indiana University Law School, March 14, 1995. At the same time, similar to the Recommendation, the EU Data Protection Directive's Article 26 provides exceptions to this general injunction. One exception concerns instances where the data subject has given *unambiguous* consent to the proposed transfer of data to a state which does not ensure adequate levels of protection. Article 26 further provides an exception permitting transfers of data where the transfer is necessary for performance under a contract between the data subject and the controller of the data. While the scope of Article 26 is still unclear and untested, the two exceptions noted may suffice to permit wire transfers to the United States, even if the United States monitors wire transfer traffic for money laundering.

to disclose personal data cannot be assumed from the intent to transfer funds.[48]

A final question involves the breadth of the exemption of Principle 5 of the Recommendation, which provides:

> Personal data collected and stored for the purposes referred to in principles 3.1 and 4.1 [so as to provide service, verify legitimacy of transactions, and manage accounts] may only be communicated in the following cases:
>
> a. in accordance with obligations laid down by domestic law;
>
> b. when it is necessary to protect the essential and legitimate interests of the body providing the means of payment;
>
> c. with the express and informed consent of the individual. . . .

Paragraph 62 of the Explanatory Memorandum notes that "obligations laid down by domestic law" extend beyond statutory duties to communicate data and court orders to cases where:

> . . . it is in the public interest to reveal personal data for the purpose of crime *prevention*. It may be the case that a body providing a means of payment strongly suspects that illegally acquired funds are being laundered through it by an account holder. Such circumstances would justify the communications of the relevant data to the police.[49] [emphasis added]

An aggressive reading of the first clause of paragraph 62 might argue that prevention of money laundering would require communicating wire transfer records to the authorities to detect money laundering, although this reading is clearly undercut by the second and third sentences, which refer to account-specific suspicion. Hence, this suggests a bootstrap problem in the case of wire transfers: the only justification for secondary processing and disclosure of personal data would be "crime prevention" but as the bank (particularly the intermediary bank) likely will be unaware of criminal conduct in advance, such potential criminal conduct will likely go undiscovered in the flood of wire transfers passing through the bank's wire room. Subsection 5.1.b suggests another interesting argument, that in order to protect the "essential and legitimate interests" of payment systems in their integrity and freedom from money laundering, disclosure might be permitted, although these arguments are scarcely certain enough to encourage foreign originating banks to risk violating data protection laws.[50]

## INTERNATIONAL LAW ENFORCEMENT EFFORTS

### Unilateral Efforts of the United States

U.S. law enforcement efforts to curtail money laundering have not stopped at the border. Al-

---

[48] This would not be true if the United States barred U.S. recipient banks from handling transfers with unidentified originators; however, the U.S. Treasury Department proposed this in its 1989 advance notice of rulemaking only to withdraw it after adverse banking industry comments. See 54 *Fed. Reg*. 45769 (Oct. 31, 1989), and 55 *Fed. Reg*. 41696 (Oct. 15, 1990).

[49] Article 13 of the EU Data Protection Directive contains a similar clause permitting member states to adopt legislative measures restricting the Directive's scope with respect to a broad class of law enforcement activities, including "the prevention, investigation, detection and prosecution of criminal offences." This clause emphasizes the difficult relationship between principles of fair information practices and the mission of law enforcement in the information age. This exemption covers Article 6(1), which sets forth principles for processing of data, but the exemption does not sanction departures from the article governing the transfer of data to third countries. Earlier, "processing" is defined broadly, to include dissemination and disclosure. The upshot is that the precise treatment of law enforcement and secondary use of data is rather unclear, and may only be settled in individual national implementation of the EU Directive.

[50] A parallel question arises in the context of the EU Data Protection Directive's Articles 3(2) and 13(d), which provide that the Directive shall not apply to the processing of personal data concerning the activities of the State in areas of criminal law; and that member states may restrict the scope of some of the Directives articles when necessary to safeguard law enforcement's mission. These provisions are by no means an unambiguous grant of an exception to law enforcement: for example, it is not clear whether Article 3(2) permits private sector disclosure of data as well as law enforcement processing. All of the initiatives seek to limit disclosure of data and it is this disclosure which is integral to any monitoring proposal.

though U.S. efforts might appear to some to be extraterritorial overreaching and a threat to the sovereignty of other states,[51] a state may properly assert jurisdiction beyond its borders in certain circumstances. One longstanding rule of international law permits a state to assert jurisdiction over its nationals no matter where they might be, if they commit a criminal act.[52] Moreover, states may assert jurisdiction even over non-nationals not present within their borders when the individual commits a crime whose effects are felt in that state. A well-known example of this is the U.S. prosecution of Manuel Noriega in South Florida for his money laundering and narcotics trafficking operations based in Panama.[53] Many foreign governments, including close allies of the United States, take issue with these extraterritorial bases of jurisdiction, out of a belief that jurisdiction ends with the territorial boundaries.[54]

The Restatement's principles are echoed in the U.S. money laundering statute, asserting jurisdiction over money laundering where

> (1) the conduct is by a United States citizen, or in the case of a non-United States citizen, the conduct occurs in part in the United States; and (2) the transactions or series of related transactions. . . . exceeding $10,000.

The United States' assertion of jurisdiction passes the muster of international legal principles as understood by U.S. courts, subject to the requirement of "reasonableness."[55] Prior to prosecution, however, targets must be identified. Unilateral efforts of the United States to investi-

---

[51] Jack Blum, S. Hrg. 103-606, p. 133. An authority on Caymanian commercial and banking law has opined that "[n]o area in international legal affairs has . . . caused more tension between governments than [the extraterritorial] investigative power of United States grand juries." Ian Paget-Brown, "Bank Secrecy and Criminal Matters: Cayman Islands and U.S. Cooperative Development," 20 *Case Wes. J. Int'l L.* 369-391, p. 379 (March 1988).

[52] The French adhere to this principle, for example. *See also* Paget-Brown, who notes that the United States may exercise jurisdiction over its citizens both within and without the United States, as well as "over all persons who purposefully avail themselves of the privilege of conducting activities within the United States and thereby invoke the benefits and protection of its laws." *Ibid*., p. 378

[53] The eminent American Law Institute publishes the Restatement of the Law series, an influential reformulation of legal rules drawn from judicial opinions and other sources. Section 402 of the Restatement of the Law (3d) the Foreign Relations Law of the United States specifies that a state has jurisdiction to prescribe law with respect to:

(1) (a) conduct that , wholly or in substantial part takes place within its territory;

(b) the status of persons, or interests in things present within its territory;

(c) conduct outside its territory that has or is intended to have substantial effect within its territory;

(2) the activities, interests, status or relations of its nationals outside as well as within its territory; and

(3) certain conduct outside it territory by persons not its national that is directed against the security of the state or against a limited class of other state interests.

Subsection (3) is often referred to as the "protective principle," for such matters as conspiracies to violate immigration/customs laws, counterfeiting and arguably money laundering, with its potential for destabilization—some sources indicate that as much as 60 percent of US funds are held abroad. The Polish Penal Code of 1969 parallels these jurisdictional bases, providing that the criminal code may be applied to offenses committed by Polish citizens wherever they might be (Article 113), as well as to offenses of non-Poles outside of the territorial boundaries of Poland, as long as the conduct either violates the laws of the other country or runs counter to the political or economic interests of Poland (Articles 114 and 115).

[54] The U.N. *Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* provides support for this view in article 2(3): a signatory state is expected to defer to the territorial boundaries of other states and not attempt to exercise jurisdiction for acts occurring there, as long as that state exclusively reserves jurisdiction. At least one commentator on multilateral cooperative efforts cautions against U.S. unilateral actions and *realpolitik* for fear that they undermine the legitimacy of diplomacy, urging instead additional U.S. efforts aimed at building new and strengthening existing international organizations and treaties to combat money laundering. Bruce Zagaris, "Developments in International Judicial Assistance and Related Matters," 18 *Denver J. Int'l Law and Policy,* 339-386, 384-85.

[55] See Todd C. Jones, "Compulsion over Comity: The United States' Assault on Foreign Bank Secrecy," 12 *Northwestern J. of Int'l Law & Business* 454-507, 486-487, *citing* the Restatement (Third), 403(2).

gate potential international money laundering (by U.S. citizens or others) have been stymied by the laws of other states.[56] This leads to the paradoxical result that although the U.S. may properly exercise criminal jurisdiction over money launderers extraterritorially, foreign bank secrecy and data protection initiatives may bar U.S. law enforcement from identifying international money launderers. Alternative avenues have been pursued, notably bilateral and multilateral agreements (addressed below), some of which expressly address the question of foreign bank secrecy as an impediment to investigations of money laundering.

## Multilateral Cooperation and Agreements

Beyond unilateral efforts at stopping international crime, the United States has both stimulated and joined international efforts to make law enforcement itself transnational, soliciting cooperation and building alliances with foreign partners. The United Nations *Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* (the Vienna Convention) was signed in Vienna on December 20, 1988 and entered into force on December 11, 1990.[57] International cooperation in pursuing money laundering has been surprisingly wide ranging and successful, if judged by the numbers of organizations created and conventions drafted. Foremost among international organizations combating money laundering is the Financial Action Task Force (FATF), created at the International Economic Summit of 1989 as a mechanism for international cooperation in fighting narcotics-related money laundering. FATF seeks to improve contact between experts and law enforcement authorities in member countries, document money laundering techniques and compile national programs targeting money laundering. FATF now has members from 26 countries.[58]

Urged on by the sense of Congress that money laundering is an international crime whose defeat cannot be achieved without involving international cooperation and agreements,[59] the United States has been instrumental in the FATF's work, especially its efforts on agreements directed at information sharing between law enforcement agencies in different countries. FATF has made 40 recommendations to its member states pertaining to money laundering. The most significant recommendations are the requirements that member states make drug money laundering a criminal offense (Recommendation 4); that member states permit banks to report suspicious transactions to the competent authorities (Recommendation 16); and that member states should not permit financial institutions to keep anonymous accounts (Recommendation 12). By the 1994 Annual Report of the FATF, all member governments permitted reporting of suspicious transactions, and 19 member governments required their banks to report such transactions. While many federal officials laud the successes of FATF in marshaling the states of the world in the battle against money laundering, at least one outside expert cautions that FATF's rhetoric outstrips its performance, pointing specifically to the slowness with which some core FATF members have implemented the forty recommendations.[60]

---

[56] See also box 6-1 in this chapter discussing the limits on the use of subpoenas to obtain records created and maintained abroad.

[57] On June 10, 1994, Colombia became the 101st signatory state to the Vienna Convention, which obligates signatory states to criminalize money laundering incident to narcotics trafficking. Article 3(b).

[58] Members of FATF include the countries of G-7 and the European Union, as well as Hong Kong, New Zealand, Australia, Singapore, Switzerland, and Turkey. Each member is entitled to representatives from its Ministries of Finance, Justice, and Foreign Affairs and its central banking system, and there are official "observers" from several international institutions.

[59] Sections 4101-4108 of the Anti-Drug Abuse Act of 1988 (Pub. L. 100-690, Title IV).

[60] Telephone interview with Bruce Zagaris, Esq., Cameron & Hornbostel, March 14, 1995.

At its most recent meeting, in 1994, the FATF explicitly broadened its mission to encompass non-drug-related money laundering. Its current goals are 1) expanding members' money laundering legislation so that money laundering prosecutions need not depend on proof of an underlying crime;[61] 2) monitoring members for implementation of the recommendations;[62] 3) monitoring developments in money laundering; and 4) encouraging the formation of regional task forces patterned after itself, such as the Caribbean Task Force and the Gulf Cooperation Council. FATF's 40 recommendations have already become the basis of rules adopted by the Caribbean Financial Task Force. The Caribbean Task Force also signed an Memorandum of Understanding with Great Britain to work on white collar crime, including money laundering, among its members.[63]

Other groups have been created in the Western Hemisphere to combat money laundering. The Organization of American States (OAS) in its 1990 meeting condemned illicit drug trafficking and money laundering and endorsed international agreements and cooperative efforts aimed at eliminating trafficking in narcotic drugs.[64] Soon thereafter, an Inter-American Commission on Drug Abuse Control (CICAD) put forth *Model Regulations Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Related Offenses.*[65] The CICAD proposals include provisions intended to remove bank secrecy as an impediment to access to banking records, as well as a proposal for civil sanctions in case of bank failure to keep records and report suspicious transactions.[66] The CICAD plan extends the definition of money laundering beyond the narcotics context.[67] It seeks to regulate broadly defined "financial institutions," prohibit anonymously held bank accounts, and require financial institutions to identify and verify their customers.[68] It also requires currency transaction reporting (with an express waiver of bank secrecy or confidentiality), prohibits structuring, and mandates suspicious transaction reporting, with safe harbor provisions for banks.[69]

In addition to these groups, the Commission of the European Communities, in 1991, issued a directive compatible with (and in some cases exceeding) the FATF recommendations.[70] The Council of Europe also passed a multilateral money laundering convention signed by 13

---

[61] Interview with Rayburn Hesse, Chief of International Narcotics Matters, Department of State, July 28, 1994. "Donor Members" of FATF (those whose donations finance the Caribbean Financial Action Task Force and other FATF activities) are the United States, the United Kingdom, France, the Netherlands, and Canada.

[62] Each year, four or five countries are chosen, with fellow members conducting detailed audits of those countries' compliance with the Recommendations. Reports of findings are issued.

[63] Fred Verinder, Deputy Assistant Director, Criminal Division, FBI, testimony in *Hearing Before the Committee on Banking, Finance and Urban Affairs*, House of Representatives, "Federal Government's Response to Money Laundering," 103rd Cong., 1st Sess., 103-40, May 25-26, 1994, p. 40.

[64] OAS General Secretariat, "Declaration and Program of Action at Ixtapa," Washington, DC, 1990.

[65] The Model Regulations have been twice endorsed by the 34 member states of the Organization of American States, (OAS) once at the annual OAS general assembly in May 1992, and more recently at the Summit of the Americas, in December, 1994. AG/doc.2916/92 rev.1.

[66] FATF's 40 recommendations became the basis of rules endorsed by the OAS.

[67] "Miami summit slights OAS proposals, agrees to more talk," *Money Laundering Alert*, Dec. 1994, p. 5; Charles A. Intriago, "OAS Unit Proposes Money Laundering, Forfeiture Laws," *North-South*, vol. 1, No. 2, August-September 1992, pp. 38-39.

[68] Article 9 ("financial institutions") and Article 10.

[69] Articles 12 through 14 and 19. In this context, "safe harbor" denotes a legislatively conferred immunity from criminal or civil liability for disclosures mandated by governments.

[70] Some sense of the gap between rhetoric and reality is evidenced by the fact that Ireland only in 1994 implemented the European Community (EC) directive by passing anti-money laundering legislation.

OECD members (and expected to be signed by four more).[71] The increased freedom of movement of people, goods, information, and currencies that will occur as the single market becomes a reality has increased concern over money laundering in Europe, and the concern is further stimulated by new awareness of organized crime, drug trafficking, and money laundering within the countries of Central and Eastern Europe. Some EU countries are now considering further legislation to combat money laundering.[72]

The Bank of International Settlements (BIS)[73] has a task force to build international cooperation in control of money laundering. International financial leaders, according to some observers, were at first hesitant to deal with the problem of abuse of bank secrecy laws. Some also feared that banks in countries such as Luxembourg had unknowingly become dependent on illicit money flowing through their accounts.[74]

The apparent cooperation is somewhat surprising in light of the lingering, if false, perception that money laundering is a predominantly American problem and the fact that possession of, if not trafficking in, cannabis and some opiates, is legal or tolerated in some of the United States' allies within the European Union. Additionally, independent of the legal status of narcotics themselves, some European states focus state efforts to prevent drug abuse on rehabilitation and education instead of on law enforcement. Beyond the narcotics context, there have been great differences in perspectives on tax evasion and avoidance, as well as some other kinds of white collar crime, impairing concerted action against all forms of money laundering. At the same time there are indications that Europe, at least, is awakening to the destabilizing threat that money laundering poses. Europol, the new multinational European police force, now has jurisdiction over money laundering in addition to its former jurisdiction over drug offenses.[75] Other states are also awakening to the destabilizing force of money laundering and its role in terrorism, arms sales and political unrest. U.S. private banking officers and regulators often meet with foreign officials and stress these less financial motives for money laundering, in seeking to create a stronger consensus for combating international money laundering.

## Bilateral Conventions and Cooperation

The United States has invested much capital in the negotiation of bilateral accords aimed at facilitating prosecutions of crime with international dimensions. Mutual Legal Assistance Treaties (MLATs) represent a considerable improvement over the older vehicles of letters rogatory and MATs (Mutual Assistance Treaties). Nevertheless, MLATs do not suffice to permit suspicionless

---

[71] "Money Laundering Experts Team Up—On and Off the Job," *Bank Management*, March 1991. Thus far only six signatory countries have implemented its terms. This signifies some of the difficulties of international cooperation, even among the closest of allies. A further example of this would be Mexico, whose legislature has been struggling to criminalize money laundering for four years now, without reaching finality. Telephone interview with Bruce Zagaris, March 14, 1995.

[72] J. Stewart-Clark, "Security Concerns in the European Community," *Police Chief*, vol. 60, No. 10, (1993), pp. 57ff.

[73] The Bank of International Settlements (BIS) was created in 1930 to promote central bank cooperation, and founded the "Basle" Committee to address international banking supervision issues, including developing a code of conduct for bank monitoring to keep financial systems free of criminal money. See Jones, "Compulsion over Comity," *op. cit.*, footnote 54, pp. 481-82, and footnotes. The Basel Statement of Principles, agreed to on December 12, 1988, are designed to fight money laundering in the banking system by promoting measures such as customer identification, cooperation with law enforcement to extent permitted by bank secrecy or confidentiality laws, and refusal to assist suspicious transactions.

[74] Brian R. Allen, "The Banking Confidentiality Laws of Luxembourg and the Bank of Credit & Commerce International," 28 *Texas Int'l L. J.*, 73-117 (Winter 1993). Luxembourg, a major banking center, now has stiff penalties for money laundering, but only three bank examiners. Verinder, *op.cit.*, footnote 63.

[75] *Money Laundering Alert*, December 1994, p. 8.

and indiscriminate access to records held abroad,[76] and in fact, unilateral U.S. efforts targeting international wire transfers may threaten the success of the MLAT process as well as other multilateral efforts detailed above.

Under MLATs, governments take on international legal obligations to provide legal assistance to each other.[77] MLATs strengthen the procedures for international cooperation, and create binding procedures, obligations and channels of communication for exchange of information and evidence in criminal investigations and proceedings.[78] The requesting country does not need to rely solely upon judicial comity to obtain the legal assistance sought (as with letters rogatory). MLATs may extend to a broader class of crimes than MATs, although they may exclude tax evasion, particularly so in treaties executed with banking haven countries, such as the Bahamas and the Cayman Islands, whose MLATs cover relatively narrow classes of crimes. The Panamanian MLAT provides a mechanism for obtaining currency transaction information accessible to the Panamanian government.

MLATs are drafted with a view towards helping ongoing investigations, and have their best success when U.S. authorities can substantiate their suspicion regarding an individual subject to foreign jurisdiction. This form of cooperation can be unwieldy: requests percolate up from the field to the Department of Justice's Office of International Affairs, thence to the Department of State and the foreign country, where the process is repeated in reverse, although MLATs may provide for requests to be forwarded directly from law enforcement agency to law enforcement agency abroad.[79]

Recently, the United States has negotiated bilateral pacts targeting money laundering; these agreements seek improved quality of information regarding currency transactions and provide avenues for sharing that information between countries. Examples of these agreements are Financial Information Exchange Agreements (FIEAs).[80] FIEAs generally require signatory countries to "ensure that. . . financial institutions. . . record currency transaction information. . . and transfer said information to their respective executing agencies. . . . "[81] and to share those records internationally. But the signatory states promise only to "provide each other the fullest measure of mutual cooperation. . . . "[82]

---

[76] The Office of International Affairs, Criminal Division, Department of Justice, avers that MLATs envision a wide range of legal assistance, even at the early stages of an investigation. Nevertheless, most configurations of a wire transfer monitoring system aim at *detecting* a possible crime so that an investigation may be opened, at which point, the MLAT could be invoked. The MLAT executed with the Cayman Islands illustrates this point. While it provides for mutual assistance in "investigation, prosecution, and suppression of [specified] criminal offenses," a party may deny a request for assistance where "the request does not establish that there are reasonable grounds for believing that the criminal offense specified in the request has been committed. . . . " *United Kingdom-United States: Treaty Concerning the Cayman Islands and Mutual Legal Assistance in Criminal Matters* (July 3, 1986), *reprinted in* 26 *I.L.M.* 536-549, Articles 1 and 3(c)(i). Moreover, the request for assistance shall include "information concerning the persons involved including, where available, their full names, dates of birth, and addresses. . . . " Article 4(2)(b). This is precisely the sort of information that a monitoring system would be attempting to discover.

[77] The first MLAT was executed with Switzerland on May 25, 1973. 27 U.S.T. 2019, T.I.A.S. No. 8302 (entering into force Jan. 23, 1977). Other MLATs have been negotiated with some bank secrecy jurisdictions, including the Bahamas, the Cayman Islands, Canada (a blocking jurisdiction) and the Netherlands (including the Dutch-Antilles).

[78] As one commentator notes, MLATs facilitate the investigation of crimes beyond producing evidence for the trials of previously indicted defendants. Napp, "Mutual Legal Assistance Treaties," *op. cit.*, footnote 14, p. 410.

[79] Zagaris, *op cit*., footnote 54, p. 352.

[80] The Anti-Drug Abuse Act of 1988 expressly urged the executive branch to negotiate these agreements, as well as the creation of the Financial Action Task Force. The first was with Venezuela in November of 1990; and Colombia, Ecuador, Panama, Peru, Paraguay, and most recently, Mexico (Oct. 28, 1994).

[81] Drawn by way of illustration from Article II, section (1) of the FIEA executed with Colombia on February 27, 1992.

[82] Article II, section (2) of the Colombian FIEA.

The utility of FIEAs will become clear in coming years, although many of the countries signing FIEAs are just beginning to police large cash transactions. For instance. Mexico, in agreeing to its FIEA with the United States, has agreed to share information that Mexican bank regulators do not currently require be held.[83] However successful these FIEAs will be in improving currency transaction information on an international level, they cannot provide a mechanism for sharing wire transfer information in real or near real time. The FIEAs require that the requesting law enforcement agency detail the charges against the individual whose currency transaction record are sought. Clearly, this does not square with one of the aims of a wire transfer monitoring system—detection beyond the investigation of existing leads.

A possible model for international cooperation in investigating international crime is provided by the efforts of the Securities Exchange Commission (SEC), which has had some signal successes in policing a similar problem in foreign anonymous financial activity in the United States—insider trading on the New York Stock Exchange through Swiss and other bank accounts. In a series of cases from the mid-1980s, the SEC persuaded Swiss authorities to disclose the identities of its customers who had initiated massive stock purchases immediately before takeover announcements. The differences between the SEC cases and wire transfers are plain, however: for one, the point of the wire transfer monitoring proposal is to identify hitherto unknown money laundering, not as in the case of the SEC, to identify the real party in interest to trades already recognized as very suspicious. The SEC has been able to demonstrate the clear violation of U.S. insider trading law, based on dramatic shifts in stock prices in advance of disclosures of material information, before requesting foreign banks and law enforcement to pierce bank secrecy.[84] This distinction aside, an interesting commonality exists regarding the extraterritorial enforcement of U.S. laws abroad. Just as money laundering has not been uniformly criminalized throughout the world, neither has insider trading, and yet the United States has been able to pierce bank secrecy.

## THE STRUGGLE OF SOVEREIGNS

At a more abstract level, this conflict between access and financial confidentiality implicates competing assertions of sovereignty: the sovereign right of the originator state to shield the data with the protections of the originating jurisdiction and the right of the United States, or recipient state, to enforce its laws and protect its borders.[85] This conflict resembles previous U.S. attempts to enforce its antitrust laws and gain access to information held internationally by multinational corporations, an effort which gave rise to blocking statutes in the first place, but with the significant difference that the wire transfer is both a transborder flow of data and an act in itself, the import or export of money. Nonetheless, as global networks bring the world closer together, they also run the risk of exacerbating conflicts between sovereignty, conflicts which prior modes of communication and finance left latent.

As noted above, the United States has always maintained its right to prosecute individuals for criminal actions committed abroad that have impacts within the territorial confines of the United States. In addition, with the successful efforts of

---

[83] Previous to signing the FIEA, Mexican authorities merely issued nonmandatory guidelines encouraging bank recordkeeping of cash transactions. Telephone interview with Joseph Myers, Asst. Legal Counsel, FinCEN, May 28, 1995.

[84] In structure, this is no different from the need to show a magistrate probable cause of criminal conduct before a search warrant is issued for a search of U.S. account records may be searched under the legislative requirements of the U.S. Right to Financial Privacy Act.

[85] When the Supreme Court looked at the foreign bank account reporting requirements of the Bank Secrecy Act (BSA) in *California Bankers Ass'n.* v. *Shultz*, the Court emphasized the plenary powers of Congress in regulating foreign commerce and expressly drew the analogy between the holding of foreign bank accounts by U.S. citizens and the crossing of international boundaries, with the implication that the sovereign has an near absolute right of inspection. 416 U.S. 21, 62-63 (1974).

FATF in criminalizing money laundering in other countries, the extradition of money launderers is increasingly possible, as the prerequisite of the alleged offense being a crime in both countries can now be satisfied. The enforcement gap remains, however, in the problem of detecting the money laundering as wire transfers pass through the United States.[86]

## CONCLUSION

Foreign bank secrecy and data protection laws present considerable barriers to the success of any monitoring system requiring indiscriminate access to wire transfer records. Moreover, U.S. efforts to unilaterally forge ahead and scrutinize wire transfer records could undermine what successes international cooperative efforts have borne, so far, such as considerable use of the MLAT procedure for aiding investigation and prosecution of money launderers and narcotics traffickers, among others. U.S. monitoring efforts also could undermine the attractiveness of the U.S. dollar as a means of international payments and disadvantage U.S. banks in the competitive marketplace of international financial services.

Should Congress decide in favor of a monitoring system, it will be essential to negotiate with the European Union and seek to obtain a policy statement that the EU Data Protection Directive is not meant to limit the ability of countries to scrutinize payment system information for money laundering.

[86] This is not to suggest that the United States is fully open to the inquiries of foreign law enforcement. In fact, ratification of MLATs has been held up in the Senate precisely out of a concern that they would permit fishing expeditions by foreign law enforcement agencies, contrary to the dictates of the Fourth Amendment. *See* Zagaris, *op. cit.*, footnote 54, p. 356. Moreover, when FinCEN negotiates international information sharing agreements, it requires that the request for BSA data be justified.

# Conclusions and Policy Options

7

Money laundering is one of the most critical problems facing law enforcement today. International crime probably cannot be controlled or reduced unless criminal organizations can be deprived of their illegal proceeds. At present, they enjoy a swift, silent, almost risk-free pipeline for moving and hiding money—international wire transfers.

OTA was asked to evaluate the possible use of computer programs based on artificial intelligence (AI) to detect money laundering through wire transfer systems. Two configurations are proposed below that singly or sequentially could meet this need and give law enforcement a potent weapon against money laundering.[1] There would be unavoidable economic and social costs.

The OTA assessment team and the project's many advisors and contributors were unable to conceptualize any AI-based configuration of technology that was likely to effectively support law enforcement and at the same time:

- would place no burden on banks,
- would involve no significant intrusions on the financial privacy of legitimate businesses and law-abiding citizens,
- would raise no troublesome issues in international relationships, and
- would not require expensive systems development.



[1] The assessment is concerned with monitoring of large-volume wire transfer systems—Fedwire, CHIPS, and SWIFT. It is not concerned with consumer-oriented electronic funds transfer mechanisms such as automated teller machines (ATMs), point-of-sale terminals, or automated clearing houses.

The most direct and conceptually simplest form of AI-based configuration—continual, automated, real-time computer screening of wire transfer traffic or records alone—would probably not be effective in detecting money laundering, OTA concluded.

The OTA team and its advisors then evaluated several alternative technological configurations. These configurations differed in technological capabilities, in possible institutional locations, in data requirements, in degree of automation, and in the likely monetary and social costs of development and deployment. They also differed in the way they would support law enforcement —whether they would identify new suspects, support investigations by uncovering evidence buried in financial records, or to do both.

These configurations offer significant promise for control of money laundering. All have obvious limitations and raise serious policy issues as listed above. Yet control of international crime appears to be nearly impossible so long as its profits can be moved with impunity through wire transfers. *Some minimum level of social and economic costs may therefore be acceptable in order to strengthen law enforcement against the threat posed by financial crime.*

Viewed in this light, two of the configurations developed in this project look sufficiently attractive that prototyping and testing should be considered under new specifically and sensitively defined statutory authority. These two technology options—"targeted access to wire transfer records" and "two level screening of wire transfer traffic"—are outlined in the concluding section of this chapter, along with two less acceptable configurations.

## MONEY LAUNDERING AND THE WORLD ECONOMY

As commerce and trade have become increasingly international and increasingly dependent on advanced communications technologies, so too has organized crime. Criminal enterprises closely mirror many legitimate, productive business practices—understandably, because both criminal organizations and business corporations are designed for financial gain. Most organized crime depends on bringing to market a product (e.g. drugs) or a service (e.g., gambling) and on returning profits to those who own and control the organization. Many criminal organizations, like legitimate businesses, now rely heavily on wire transfers to move funds swiftly and securely between banks around the world. South American drug cartels, for example, are organized and behave like multinational corporations. Because attempts to interdict the flow of drugs into the United States have met with only limited success, it has become increasingly desirable to stop the flow of profits to cartel leaders and to seize the earnings and assets of participants in all phases of the drug trade. The same enforcement strategies are promising in attacking other criminal activities, including racketeering, white collar fraud and embezzlement, and terrorism[2] (see box 7-1).

Law enforcement agencies have usually attacked organized crime by attempting to incarcerate its workers.[3] The newer, complementary strategy of disrupting its business practices by stemming the flow of profits and seizing assets requires more information about the behavior and vulnerabilities of criminal organizations. Law enforcement must of necessity match the growing

---

[2] Terrorism, unlike the other crimes mentioned, is usually not aimed at financial gain. Terrorists may smuggle or wire money into this (or other) countries to support themselves and their activities, however, and like other money launderers wish to conceal both the origin and the destination of the funds.

[3] Some experts have commented that the targeting of individual criminals and "individual-oriented prosecutions" may only "help to open the promotion ladder within organized crime groups, moving new individuals into management positions while the group and the crime matrices they engage in continues." Peter A. Lupsha, "Steps Toward a Strategic Analysis of Organized Crime," *Police Chief*, vol. 47 No. 5, May, 1980, as quoted and expanded on by Malcom K. Sparrow, "Network Vulnerabilities and Strategic Intelligence in Law Enforcement," *Intelligence and Counterintelligence,* vol., No. 3, 1991, p. 256.

## BOX 7-1: Terrorism And Money Laundering

Terrorism IS "deliberate employment of violence or the threat of violence by sovereign states, or by subnational groups possibly encouraged or assisted by sovereign states, to attain strategic or political objectives by acts in violation of law Intended to create a climate of fear in a target population larger than the civilian or military victims attacked or threatened."[1] Increasingly, terrorism has religious, racial, or ethnic as well as political motivations It may be purely domestic, as is suspected to be the case in the Oklahoma City explosion in April 1995, or the terrorists may come from other countries. Terrorism may range from one or a few violent actions meant to make visible some cause or grievance, to continuing warfare against an entrenched regime.

Terrorists, as well as drug traffickers and other criminal organizations, need to launder money It takes money for weapons and explosives It takes money to get terrorists to their targets, and then into hiding. Continuing subversive organizations also need money for maintaining networks, and for the support and protection of active members, their dependents, and their survivors According to one expert, the amount of money that the Irish Republican Army has required to support its nonactive units and to contribute to the families of those killed or imprisoned, is "significantly greater than the funds required for direct action."[2]

This money must be raised and hidden, and in many cases must be carried or sent across national boundaries. Both the origin and the destination of the funds must be concealed. Individuals or small groups may try to handle this themselves, but it is thought that larger and more highly organized terrorist organizations seek the help of specialized money launderers, whom they may contact through organized crime.[3]

---

[1] U.S. Congress, Office of Technology Assessment, *Technology Against Terrorism: the Federal Effort*, OTA-ISC-481 (Washington, DC U S Government Printing Office, July 1991, p 16-17) This definition is derived from comparison of several definitions used by the U S Department of State, Department of Defense, and CIA See also, U S Congress, Off Ice of Technology Assessment, *Technology Against Terrorism: Structuring Security,* OTA-ISC-511 (Washington, DC U S Government Printing Office, June 1992)

[2] Dr. Barry A K Ryder, in a Memorandum on Organized Crime submitted to the Home Affairs Committee of the British House of Commons, Nov 16, 1994, reproduced in *Money Laundering, Forfeiture, Asset Recovery Offshore Investments, and International Financial Crime,* a Conference Course Book, Feb. 23, 1995 Oceana Publications, p 129

[3] Some law enforcement experts argue that formerly sharp distinctions between traditional criminal organizations and terrorists may be breaking down (Ryder, op. cit., footnote 2) Terrorists not only need the money laundering expertise that criminals have or know how to contract for, they are also sometimes willing to engage in non-political criminal activities to raise funds for terrorist activities. This leads them to collaborate with criminal groups, but it may also make them competitors Criminals, on the other hand, may adopt some of the terrorist tactics, such as threat of product contamination, as a means of extortion Either group may have access to weapons and ammunition—smce the breakup of the Soviet empire, even to weapons of mass destruction—and maybe willing to sell them to the other,

*(continued)*

sophistication of international criminal activities. Successful law enforcement now depends on financial analysts as well as agents, databases as well as weapons, and strategic assessments as well as raids. The use of advanced information technologies and computerized databases as a shared resource among several law enforcement agencies, is on the cutting edge of modern law enforcement.

All of the money generated by criminal organizations cannot—as cash—be efficiently used for organizational maintenance or safely distributed as profits. In today's world of checks, credit cards, and electronic funds transfer, a large bundle of bills immediately draws the suspicion of bankers and the attention of law enforcement agents.

The fastest way to move millions of dollars out of sight of law enforcement is to use international wire transfers, even though this requires first placing the money into a bank. With approximately 700,000 wire transfers every day, illegal transfers

## BOX 7-1: Terrorism and Money Laundering (Cont'd.)

Under the International Emergency Economic Powers Act[4] and related legislation,[5] the President can direct U S financial institutions to freeze the assets and block the accounts of persons and organizations belonging to designated hostile or renegade countries The regulations implementing this act, which currently applies to Cuba, Libya, Iraq, Haiti, and the Federal Republic of Yugoslavia (Serbia and Montenegro), are administered by the Dept of Treasury's Office of Financial Assets Control (OFAC) Over 2,000 people, groups, and companies are on the OFAC list of "Specially Designated Nationals and Blocked Persons "

On January 23, 1995, President Clinton ordered that the assets of 30 Arab and Israeli groups be frozen, "in an attempt to prevent terrorist groups or their supporters in the United States from using the American banking system to finance terrorism. "[6]

Administration officials said that they did not know whether these groups actually had assets in the United States However. some officials estimated that as much as 30 percent of the financial aid from supporters intended for Hamas, a Palestinian terrorist group, may pass through the United States [7] In late 1994, Israel sentenced Mohammed Salah, a used-car salesman from Bridgeview, Ill., for carrying orders and thousands of dollars to Hamas leaders in Israel and the occupied territories

Terrorism is not listed in U S anti-money-laundering statutes as one of the "predicate crimes" defining money laundering, although FBI officials point out that terrorism usually involves murder, kidnapping, robbery, or extortion all of which are predicate crimes for money laundering As a result of the Oklahoma City and World Trade Center bombings in the United States, OTA has been told, proposals are being framed to add terrorism to the list of money laundering predicate crimes

[4] 50 U.S.C. §§ 1701-06

[5] Trading with the Enemy Act, 50 U.S.C. App. §§ 1-44, Iraq Sanctions Act, Pub L 101-513, 104 Stat 2047-55 United Nations Participation Act, 22 U.S.C. § 287c, International Security and Development Cooperation Act, 22 U S C 2349 aa-9; 18 U.S.C. § 1001

[6] Elaine Sciolino, "Bankrupting Terror, " *The New York Times,* Jan 26, 1995, Sec A

[7] Sciolino, op. cit., footnote 6

SOURCE: Office of Technology Assessment, 1995

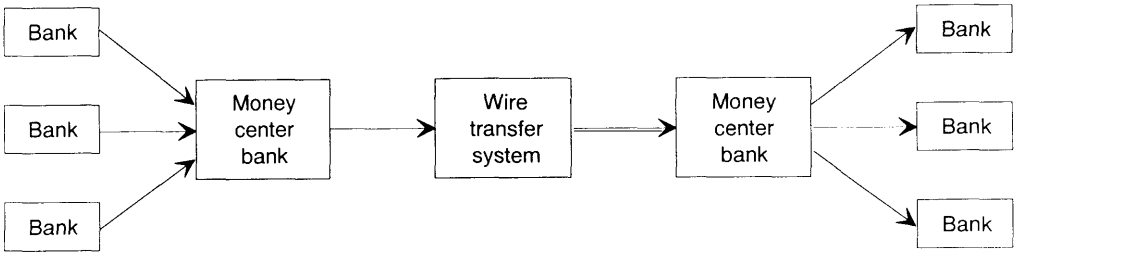
are easily hidden. Their audit trails are obscured within enormous databases that are generally safe from law enforcement investigators. By comparison, physically smuggling cash and even paper-based monetary instruments across national boundaries—although often successful—is slow and unacceptably risky.

Wire transfer systems—Fedwire, CHIPS, and SWIFT[4]---are open conduits for the two-way flow of illegally gained money from the United States to drug kingpins and back to the United States for investment or purchases. *Making these conduits less hospitable to money launderers is therefore a high priority. At the same time, the efficiency of wire transfers for the conduct of American and world financial transactions must be maintained.*

Inspection of the traffic through wire transfer systems, or ready access to wire transfer records after transmission, could make it possible to identify otherwise unsuspected operations or collect additional evidence against suspects (figure 7-1 ). Real-time inspection has been assumed to be impractical because of the speed and volume of transmission, and because it is critically important

[4] See chapter 2 for description of these systems. As discussed in Chapter 2, SWIFT is not technically a wire transfer system but a communications system for transmitting book transfer instructions; Fedwire is a domestic transfer system but facilitates transfers among and between U.S. banks and U.S. branches of foreign banks which have the effect of international transfers.

Figure 7-1: Existing Wire Transfer System




SOURCE Off Ice of Technology Assessment, 1995

that legitimate wire transfer traffic not be impeded. After-the-fact inspection of wire transfer records is also difficult; the databases containing them are almost unmanageably large, and individual records have been difficult to retrieve. Once found, the records have been relatively uninformative because of the sparse information contained in a transfer message.

The Department of Treasury and the Federal Reserve System have taken the first step in improving this situation with wire transfer recordkeeping regulations that will take effect in January, 1996. These regulations, discussed in chapter 2, will require that a wire transfer message carry essential information (originator bank, beneficiary's bank) in all segments of its journey. This will make it somewhat easier for law enforcement to find and retrieve evidence to be used against suspects, but it offers no help in detecting unsuspected operations. The existence of the transfer and some facts about it must be known in advance, in order to make retrieval possible and legal.

To overcome the operational difficulty of monitoring wire transfers to detect money laundering operations, several kinds of advanced computer capabilities using artificial intelligence (AI) have been proposed. These were explored in chapter 4. Chapters 1 through 3, in describing the process of electronic money laundering and its control, noted explicitly and implicitly some of the requirements for such systems, and some of the constraints on their development. Chapters 5 and 6 pointed to still other problems. In summary, these constraints include:

- problems in characterizing electronic money laundering—in other words, how to specify what the computers should look for;
- problems of designing systems that meet the needs of, and will be effectively used by, law enforcement agencies;
- concerns about individual financial privacy and corporate confidentiality;
- international considerations, especially foreign bank secrecy and data protection laws;
- concern for the burdens that may be laid on financial institutions and thence on the strength and competitiveness of U.S. payments systems and clearance mechanisms; and
- the costs of developing and deploying systems compared to the possible benefits accruing to law enforcement.

Most of these constraints are summarized below with frequent reference to earlier chapters for more detail; the last two are discussed in describing specific systems under consideration. This chapter lays out several alternative technological and institutional configurations for consideration by Congress and executive agencies. The strengths and weaknesses of each alternative configuration are described to provide a range of options for public policy makers. These options include possible prototyping and trial of one or more configurations.

## WHAT WOULD A COMPUTERIZED MONITOR LOOK FOR?

There are nearly 500,000 wire transfers daily on Fedwire and CHIPS with a total value of about $2 trillion, and some 200,000 more messages on SWIFT initiating book transfers in the United States. OTA estimates that about 0.05 percent of the transfers represent money laundering.[5] The one-in-two-thousand transfer that is illicit is difficult or impossible to distinguish from ordinary business transactions. Some reasons for this are as follows:

- Money laundering operations usually are kept separate from other parts of the criminal organization (e.g., the drug handlers) so that there are few identifiable links between money flow and the activities that generate the money.
- Many money launderers use shell corporations or front companies that cannot easily be distinguished from legitimate enterprises.
- Legitimate corporations and financial institutions, as well as money launderers, use banks and hold corporations in "tax haven" and "bank secrecy" countries, for a variety of reasons.
- Money launderers often use certain kinds of specialized bank accounts for cash aggregation, disbursing funds, or receiving funds before or after wire transfer; these bank accounts having been designed for similar uses by legitimate corporate customers of large banks.
- Many practitioners of money laundering are professionals, often accountants or lawyers, well versed in sophisticated techniques of cash management, tax reduction, currency trading and exchange, etc., and may serve both legitimate and illegal clients.
- Banks have difficulty in applying "know-your-customer" indicators to users of wire transfers.[6]

Not only is it difficult to recognize a specific wire transfer as illegitimate or suspect, but it is also difficult to recognize money laundering activity. *Law enforcement agents, bankers, and bank regulators readily admit that they cannot at this time supply the sets of indicators that would allow an expert system reliably to tag suspect wire transfer activity.* Constructing reliable "profiles" of money launderers or money laundering operations encounters several problems:

- differences in tactics according to the nature of the underlying crimes: drug-related, gambling and prostitution, embezzlement, fraud or terrorism;
- differences in tactics according to ethnic, cultural, or geographical source (South American drug cartels, the Asian heroin trade, Vietnamese gangs, Italian Mafia, U.S. Mafia, etc.); and
- the readiness of money launderers to switch quickly among alternative modes of money laundering—for example, smuggling, wire transfers, use of false invoicing—according to what they perceive to be the current allocation of attention and resources by law enforcers.

## DESIGNING SYSTEMS FOR USE BY LAW ENFORCEMENT

Any monitoring system that is developed must have high credibility with field enforcement agents or it will tend not to be used. This is a serious problem, because screening systems applied to wire transfer records are likely to produce a high proportion of false positives (see box 4-5 in chapter 4). This could reduce the system's credibility, at least for some time, and the necessity of disproving the false positives and sorting out fruitful leads would meanwhile consume scarce resources.

---

[5] See box 4-4 for details of this estimate.

[6] Most wire transfer instructions reach the funds transfer department of a money center bank electronically from the computers of branches, other banks, or corporate customers. Wire transfers by individuals are generally originated at a local branch office of the bank, but money launderers are likely to use several branches so that their patterns of behavior do not become apparent. In part for these reasons, voluntary reporting of suspicious wire transfers has not proven effective in the past.

From 1970 to 1995, Congress developed a legislative framework for attacking money laundering, responding to the problems encountered in law enforcement by enabling progressively more stringent enforcement strategies:

- first, creating an audit trail for certain kinds of transactions through recordkeeping and reporting requirements imposed on financial institutions and some other commercial establishments;
- secondly, by directly criminalizing money laundering and complicity in money laundering;
- subsequently, by increasing the penalties both for money launderers, and for financial and other institutions that fail to comply with reporting requirements; and
- finally, by extending civil asset seizure and forfeiture provisions to money laundering proceeds.

At the federal level, as described in chapter 3, efforts to control money laundering are distributed primarily among four law enforcement agencies and the Financial Crimes Enforcement Network (FinCEN), a financial crime data analysis and intelligence agency which is also responsible for administering the Bank Secrecy Act.

The Federal Bureau of Investigations and the Drug Enforcement Administration, both part of the Department of Justice, have their primary focus on underlying crimes such as racketeering and drug trafficking, but have added strong attention to money laundering control. The Internal Revenue Service's Criminal Investigations Division and the U.S. Customs Service, both in the Treasury Department, focus directly on money laundering because many financial crimes constitute evasion of taxation and are considered a direct threat to the integrity of the U.S. dollar. In spite of these subtle differences, all of these agencies have field offices and agents, conduct undercover operations, mount raids, and apprehend criminals; all four also increasingly use databases, intelligence analysts, and computer-assisted analysis.

FinCEN, although located in the Treasury Department, supports all of these agencies and also local and state enforcement agencies, with analytic services based on advanced information technology. FinCEN assesses Currency Transaction Reports (CTRs) from financial institutions, using AI and other techniques that would be appropriate for monitoring wire transfers. FinCEN therefore gets detailed consideration in the options laid out below.

The interaction of these two aspects of money laundering control—direct enforcement and intelligence—creates tension and difficulties both among the agencies and within each agency. Direct enforcement must protect its undercover operations and informants through close control of information and guarantees of confidentiality. By contrast, intelligence and strategic analysis often relies on sharing of data, interactive analysis, and dissemination of information. Although both the willingness and the ability to cooperate among agencies has greatly increased in recent years, tensions remain. Field agents tend to disparage the work of intelligence units, both those within their own agency and FinCEN, and to resist any efforts to reallocate resources from undercover operations to strategic analysis or data analysis. To counter this, new mechanisms for detecting electronic money laundering must be highly credible to law enforcement agencies and their field agents.

## PRIVACY AND CORPORATE CONFIDENTIALITY

Advances in technology often challenge the socially accepted balance between the power of the state to enforce laws and the autonomy and privacy of citizens. Communications and computer technologies in particular may inadvertently provide new opportunities for crime, new ways of concealing crime, and new ways of evading apprehension. On the other hand, they also increase the government's power for intrusive surveillance of all citizens.

Supreme Court Justice Sandra Day O'Connor recently expressed this sense of a balance to be maintained:

> In recent years, we have witnessed the advent of powerful, computer-based recordkeeping systems that facilitate arrests in ways that have never before been possible. The police, of course, are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.[7]

Money launderers now take full advantage of the efficiency of modern funds transfer systems. If law enforcement agencies are given ready access to wire transfer data in an attempt to redress the balance, for every money launderer identified or suspect investigated, thousands of corporations and individuals would see their financial privacy reduced. How the balance between law enforcement and privacy is restruck is thus an important factor in assessing potential monitoring systems.

In striking this balance, several points should be considered that undermine the claim to financial privacy in wire transfer records. First, Congress has plenary authority over the stream of interstate and international commerce. Second, the Supreme Court has expressly noted the reduced privacy interests in financial records maintained at banks as compared to such things as books, pamphlets, and private papers (see chapter 5). Finally, the U.S. Customs Service has virtually unlimited authority to search people, goods, and documents crossing U.S. borders. The right of a nation to protect its borders and the integrity of its money supply arguably extends to international wire transfers as well. Thus, the United States has a particularly strong case for the power to scrutinize wire transfers that cross its borders. In fact, section 1515 of the Annunzio-Wylie Anti-Money Laundering Act of 1992 grants the Department of the Treasury the authority to "request" records of international wire transfers from banks.

Disclosure to law enforcement agents of bank records of domestic transfers now requires some form of judicial process. Most of the technological options discussed below call for a more general grant of access to wire transfer records for law enforcement. The intrusion might be minimized by a legislative regime restricting the uses of the data and further disclosure, limiting the duration of retention, and providing safeguards for data security. A limited means of granting increased access to domestic wire transfers would be to confer subpoena authority on FinCEN (see box 7-2). An innovative means of safeguarding the confidentiality interests of corporations, the parties predominantly using wire transfer systems, would be to permit expedited dispute resolution for claims of economic detriment.

Subsequent manipulation of the wire transfer records, relating them to financial, personal, or corporate data in other databases, is a form of computer matching, to which many people vigorously object on grounds of privacy.[8] Most of the configurations also call for retaining wire transfer data on subjects classified as "suspicious," many of whom will turn out to be innocent. This would create a new database within the government, with the attendant concerns about inaccurate or obsolete information and use of information beyond the initial purpose for its collection.

Existing federal and state legislation and judicial pronouncements on data protection have been likened to a "patchwork quilt." The Supreme Court has ruled that the Fourth Amendment does

---

[7] *Arizona* v. *Evans, (*Docket No 93-1660) (March 1, 1995), Justice O'Connor, with whom Justice Souter and Justice Breyer join, concurring.

[8] The Computer Matching and Privacy Protection Act (Pub. L. 100-503) limits government computer matching, although law enforcement enjoys an exemption from its dictates. (5 U.S.C. §522a(a)(8)(B)(iii))

## BOX 7-2: Subpoena Power

Conferring subpoena power upon FinCEN or another federal agency to demand wire transfer records represents a considerable departure from the traditional model of criminal investigations-the grand jury of citizens issuing subpoenas and indicting targets Nonetheless, federal administrative agencies have accumulated a broad variety of subpoena and summons powers in order to ensure compliance with their regulations and orders As some violations of agency regulations may also involve criminal conduct, the distinction between civil and criminal investigations has blurred In addition, some civil penalties have grown so large as to become nearly criminal in nature For Instance, the Department of Justice has subpoena authority to investigate potential civil violations of law carrying penalties of a million dollars a day As a result of this blurred distinction between civil and criminal investigations, some have called for consolidating the form that subpoenas take.[1]

### Subpoenas in a Nutshell

All subpoenas must navigate constitutional and legislative requirements Generally courts will enforce administrative subpoenas where the agency can make the *prima facie* showing that 1 ) the investigation is pursuant to a legitimate purpose; 2) the inquiry is relevant to that purpose, 3) the information is not within the agency's possession; and 4) the administrative procedures in the authorizing statute are followed Next, negative challenges to the subpoena must be withstood

The U.S. Constitution guards against overly broad, indefinite subpoenas the items sought must be described with particularity A grand jury subpoena has been quashed where the court found that there was no reasonable possibility that the subpoenaed materials would produce Information relevant to the grand jury Inquiry. *United States v. R. Enterprises,* 498 U.S. 292 (1991). Likewise in the civil context, a federal appellate court has quashed a subpoena issued by an agency evaluation before it had Independently concluded that a violation was likely. *SEC v. Wheeling-Pittsburgh Steel Corp., 648* F.2d 118 (3rd Cir. 1981) *(en bane)*

Another line of cases has spoken to the complex relationship of civil and criminal investigations, in the context of challenges to Internal Revenue Service (IRS) civil summonses These decisions have prohibited the use of the civil summons once a matter has been referred to the Department of Justice for possible criminal proceedings Congress later codified this rule in the Internal Revenue Code [2] Speaking generally, use of IRS civil summonses has been enforced by the courts where the IRS is deemed not to have a "solely" criminal purpose in issuing the summonses [3] This would appear to present a victory of the traditional grand jury model of subpoena authority in solely criminal investigations, but subpoenas issued by a FinCEN would also be aimed at uncovering potential targets for civil forfeiture.

---

[1] Hughes, Graham, "Administrative Subpoenas and the Grand Jury Converging Streams of Criminal and Civil Compulsory Process," 47 *Vanderbilt L. Rev* 573-672 (April 1994) Legislation has increasingly conflated the form of subpoena–-see, e g the Electronic Communications Privacy Act, at 18 U S C 2705, adverting to the alternate use of either a grand jury subpoena or an administrative subpoena. Look also to the fact that the Right to Financial Privacy Act expressly permits the use of "available" subpoena authority to gain access to financial records, without requiring the use of a grand jury subpoena

[2] 26 U.S.C. 7602(c)

[3] Others take the diametrically opposing position: only the gravity of criminal violations justifies the use of subpoena authority Support for this proposition is also found in RFPA, at 12 U.S.C. 3405, specifying that administrative subpoenas will permit disclosure of records covered by RFPA only if "there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry." This provision also acknowledges that administrative process may be used for criminal investigations.

(continued)

## BOX 7-2: Subpoena Power (Cont'd.)

Despite these limitations on subpoena powers, it should be noted that courts have never suggested that a subpoena must be supported by probable cause, particularly for bank-held records [4] In the floor debate incident to the passage of the Right to Financial Privacy Act (RFPA), two senators debated the requirement of probable cause, rejecting it as a legislative standard for access to records covered by RFPA.

While probable cause is not required, it might be argued that the grand jury still fills a vital role as an intermediary, a panel of peers Interposed between the target of the Investigation and the investigating constabulary, to temper possible excesses But the federal right to an Indictment by grand jury does not connote a right to criminal investigation mediated by the grand jury. That is, "nothing in the tradition of grand jury practice supports the exclusion of material gathered by civil process."[5] Hughes stresses that the grand jury's role in indictment serves as the ultimate trammel on prosecutorial abuses in protecting the liberty of the innocent. [6]

### Electronic Subpoena

In order to facilitate investigations and streamline the often slow process (also, reduce costs of bank compliance once start-up costs are absorbed), it has been proposed that FinCEN be endowed with subpoena power that could be exercised electronically, This creates several problems First, banks may resist the electronic subpoena, necessitating drawn-out and costly enforcement actions in court, however, should the federal government prevail, further bank resistance might be quelled, Second, subpoenas currently served upon third parties, such as banks, generally require notification to the investigation's target and opportunity to quash. [7] RFPA provides for delayed notice, upon judicial finding that 1) the investigation is within the lawful jurisdiction of the agency seeking the record, 2) there IS reason to believe that the records are relevant to a legitimate law enforcement Inquiry, and 3) there IS reason to believe that such notice will result in destruction of evidence, flight or otherwise Jeopardy to the investigation.[8] In the case of wire transfer records sought by electronic subpoena, there would neither be opportunity to quash the subpoena on the basis of irrelevance or lack of a legitimate law enforcement purpose, nor the requirement of a showing that the records sought might jeopardize the investigation if notice is provided With the electronic subpoena, neither a grand jury nor the judiciary itself would temper the administration of law enforcement investigations, a significant cost undermining the benefit of rapid access to wire transfer records Of course, the mild remedy of delayed notice could be required, as it is in RFPA's section 3409(b),

---

[4] "Since no Fourth Amendment interests of the depositor are implicated here, this case IS governed by the general rule that the Issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution IS contemplated at the time of the subpoena IS issued " *United States v. Miller,* 425 U S 435, 444 (1976)

[5] Hughes, 47 *Vanderbilt L. Rev.* at 625-26 See also, *Costello v. United States 350 U.S. 359, 362 (1956).*

[6] *Ibid.*

[7] See, e.g. RFPA, 12 U.S.C. 3405(2) (for administrative subpoenas) 26 U S C 7609(a) and (b) provide the special procedures for I.R.S. third party summonses, although subsection (g) provides an exception in circumstances where there IS reasonable cause to "believe the giving of notice may lead to attempts to conceal, destroy or alter records relevant to the examination "

[8] 12 U S C 3409(a)

SOURCE Office of Technology Assessment, 1995

not prohibit the government from obtaining financial information that has been revealed to a bank: an individual or corporation has no legitimate expectation of privacy in this financial information.[9] Congress partly compensated for this by passing the Right to Financial Privacy Act (RFPA), but courts have held that this act does not protect wire transfer information at all stages of its transmission. Nor does its protection extend to corporations and large partnerships. Most wire transfer users are corporations, who fear the leakage of sensitive financial information to their competitors.

The Electronic Communications Privacy Act (ECPA) limits government access to wire transfer records, although this protection applies only until the records are transferred from electronic form to another media.[10] ECPA specifically bars a service provider from monitoring communications for evidence of criminal conduct. This provision would have to be changed or new legislation written to allow the proposed wire transfer monitoring.

Some argue that if wire transfer users are given effective notice of wire transfer monitoring or record searching, their continuing use of wire transfer systems would imply consent. Others say that intrusion is minimized because there are alternative forms of payment, e.g., checks. In practice, however, this argument lacks merit: the pace of trading in world markets now requires almost immediate transfer of funds. As alternative modes of electronic payment, e.g., "digital cash," develop, whatever precedents are set for access to wire transfers might also be applied to these alternatives. If not, digital cash or "the electronic purse" may provide another channel for dirty money, so that monitoring of wire transfers will no longer be effective (see box 7-3).

## INTERNATIONAL CONSIDERATIONS

Law enforcement access to international wire transfer data raises additional questions about several things:

- foreign bank secrecy and blocking laws,
- foreign data protection laws governing the trans-border flow of data or precluding inclusion of some information on wire transfers,
- potential effects on the international flow of capital and on the role of the dollar in international payment systems, and
- issues related to unilateral, bilateral, and multilateral arrangements for cooperation in crime control.

While U.S. law enforcement currently may subpoena records of international wire transfers held by U.S. banks, bank secrecy laws and blocking laws in many countries may limit the useful information carried on incoming wire transfers.[11] This problem is of growing interest to law enforcement, as much money wired overseas for laundering is thought to flow back to the United States, also by wire transfer, for investment. Some countries with strong bank secrecy laws are now more willing to cooperate with international law enforcement. This cooperation through international bodies such as the Financial Action Task Force (FATF) and the United Nations, could be imperiled by aggressive unilateral law enforcement efforts (see chapter 6).

The practical problem remains that banks in secrecy jurisdictions or data protective countries may be compelled to protect their customer's anonymity by not identifying the originator on a wire transfer message, thus frustrating some screening systems. Even if the United States, as was once proposed, refused to permit its domestic banks to

[9] *United States* v. *Miller,* 1976. Some states (e.g., California) extend constitutional protection to financial privacy (see chapter 5).

[10] Fedwire converts the information to microfiche after six months, while money center banks may maintain the records on optical disk for up to five years.

[11] Bank secrecy laws prohibit banks from releasing customer information to third parties; blocking laws prevent foreign law enforcement or judicial authorities from obtaining access to protected data.

## BOX 7-3: Digital Money

A growing number of technologies are being devised for transferring payments over electronic networks, These technologies, known under the general rubric of *digital money,* may dramatically alter the environment within which policies on money laundering and wire transfers must operate, Although the use of digital money is in its infancy, its use is likely to grow dramatically in the next several years, Policy makers contemplating action on money laundering should consider how their policies will operate in the world of digital money that is likely to emerge within the next five years,

Digital money offers both advantages and pitfalls, The new capabilities offered by the technologies could facilitate electronic commerce, assist the growth of new types of businesses, and allow consumers to preserve privacy when they desire, At the same time, it could render existing policies and laws obsolete by altering who can provide financial services, what records those services generate, and whether those records are accessible to law enforcement,

**Technologies**

Most technologies for digital money are designed to escape limitations or drawbacks of existing payment methods. For example, cash payments cannot be conducted over electronic networks and large payments require handling bulky paper currency, Credit card payments can be made with only a single number (allowing fraudulent use) and identify the person making the payment (perhaps sacrificing individual privacy), Payments using checks cannot be made over electronic networks, can be counterfeited, and identify the person making the payment,

Some approaches to electronic payment make minimum modification of existing payment schemes. [1] For example, one approach involves the escrow and verification of conventional credit card Information. This scheme is currently in use by First Virtual Holdings, Other systems are electronic analogues to conventional payment methods, For example, NetBill is essentially a credit card service customized to support electronic commerce. NetCheque is essentially a method of sending electronic checks.

Methods based on credit cards and checks, however, have several disadvantages, First, payments with credit cards and checks provide vendors with information about the buyer This information can be used by vendors to build up detailed profiles of their customers, particularly when the vendor can purchase additional information to correlate with transaction records, In contrast, transactions carried out with cash do not provide the seller with identifying information, Privacy advocates see this as a key advantage of cash transactions, Second, credit cards and checks both require vendors to extend credit to buyers and enter into a relationship with third parties such as the buyer's bank or credit card issuer, In contrast, cash is "legal tender for all debts, public and private, "

[1] The specific schemes mentioned in this box (and their Internet uniform resource locators (URLs)) are: First Virtual Holdings, Inc., a corporation established in 1994 (http://www.fv.com); NetBill, developed by researchers at the Information Networking Institute at Carnegie Mellon University (http://www. ini.cmu.edu/netbill/); NetCheque, developed by researchers at the Information Sciences Institute at the University of Southern California (http://nii-server.isi.edu/info/NetCheque/); DigiCash, a Dutch corporation (http://www.digicash.com/).

*(continued)*

process incoming wires that do not name the originator, foreign banks could still insert a fictitious name.

Banking haven countries—for example, the Cayman Islands—that offer secrecy and tax avoidance to bank account holders create a hospitable base for money launderers. But banking havens have legitimate as well as illegitimate uses and increasingly play an important role in the world economy. Large corporations and banks le-

## BOX 7-3: Digital Money (C

Electronic analogues to physical currency are in development. For example, Digicash's ecash allows payment in many of the same ways as physical currency. Every user of ecash must hold an account in a digital bank on a network. When users withdraw money from their account, their computers generate a unique serial number for each digital "token" that represents a unit of currency. Those tokens are sent to the user's bank, which withdraws funds from the users account, authenticates each token by encoding the serial number with its private key, and returns the tokens to the user.[2] The authenticated tokens can now be transferred (much like physical currency) to a vendor. By using the bank's public key, the vendor can verify the authenticity of the tokens. The vendor then transfers the tokens to the bank which verifies that the tokens have not already been redeemed and credits the vendor's account.[3] Digicash's ecash is currently being tested on the Internet prior to releasing the fully operational service. As of January 1995, about 5,000 people from nearly 50 countries had applied to participate in the test.

Other schemes for digital cash involve the use of *smart cards*. Smart cards are the size and shape of standard credit cards, but contain a tamper-resistant electronic chip and magnetic storage. The card acts as an electronic storage and processing device for electronic tokens. To deposit money onto the card, a user would insert it into a machine similar to an automatic teller. To pay for goods or services, the users would transfer tokens from their cards to a vendor's storage device (another card or a different type of device incorporating the tamper-resistant chip). The chips ensure that electronic tokens are not duplicated or spent twice.

### Effects

Digital money will make the Internet more attractive to vendors and to consumers. Digital money will facilitate the sale of information over networks by allowing for the contemporaneous payment for textual, photographic, audio, and video data as they are transmitted. This will facilitate electronic publishing by providing profits to the creators of intellectual property. Some forms of digital money may also offer possibilities beyond those of paper money, such as providing a permanent link to the legitimate owner or allowing the imposition of constraints on its use (e.g., parents could prevent children from using the digital money on cigarettes, or governments could limit the use of welfare payments).

Unfortunately, digital money could also facilitate money laundering. The problem of smuggling bulky paper currency potentially evaporates: if millions of dollars may be stored on a smart card, then an entire year's worth of drug revenues might only fill a wallet and could be transported quickly and securely. If the digital money can be accessed via computer, then there need be no physical transportation at all. Funds accumulated in one country could be accessed and downloaded in another. Digital money may render the Currency Transaction Report (CTR) irrelevant: if transactions are as simple and anonymous as exchanging paper currency, then traffickers in narcotics may never need to place their funds in banks at all. At the same time, existing laws and regulations may suffice to control the possible criminal use of digital money: transactions over $10,000 could require generation of an electronic record, as is currently the case with paper currency.

---

[2] Like many network payment schemes, digital cash relies on *public key encryption.* Public key encryption functions by using two keys A key is a long string of letters and numbers that can be used to encode a message. A message encoded with one key can only be decoded with the other key (and vice versa). One key cannot be computed from the other key. Users make one key, called the *public key,* available to anyone who wants to send them a message. Users then decode messages they receive by using the other key, called the *private key.*

[3] Ecash does not reproduce one key advantage of physical cash, the ability to accept payment from consumers without having to extend credit, Vendors must check with a digital bank before accepting payment to determine whether the tokens have already been used and must immediately redeem electronic tokens at the bank.

## BOX 7-3: Digital Money (Cont'd.)

Advocates contend that electronic payment systems are relatively safe from criminal uses, For example, Digicash argues that their form of electronic cash (ecash) IS "totally useless" for drug sales, First, the anonymity of ecash IS present only for the buyer, not for the seller of goods, Any one drug buyer could Identify drug sellers if the buyer decided to cooperate with law enforcement authorities Second, ecash must be deposited with a bank after a single transaction, it cannot be used repeatedly in the same way as physical currency In theory, this would allow banks to report large deposits under Bank Secrecy Act (BSA) requirements. Neither of these mechanisms guarantees legal transactions, but they do provide some potential for identification and Investigation of illicit activities, Second, according to David Chaum, tire CEO of Digicash and a major researcher in field, some digital cash schemes could allow "tiered" privacy providing a level of anonymity appropriate to the transaction, Video rental and book purchases could provide full anonymity to buyers, purchases of handguns or explosives could require full disclosure on the part of the buyer; other purchases could fall somewhere in-between [4]

WiII digital money's widespread use undercut the utility that law enforcement could derive from wire transfer Information? If wire transfers are monitored, presumably the criminal element could shift to using digital money, with the result that confidentiality in the wire transfer system might be compromised for little law enforcement benefit. In addition, digital money networks might then become attractive to some corporate users, providing digital money with an unfair competitive advantage over wire transfer systems Alternatively, law enforcement may seek to monitor digital money transactions as well as wire transfers Today's legislative and regulatory decisions about wire transfers may set a precedent for the monitoring of digital money, although it would appear that digital money networks wiII serve a distinct clientele with more frequent transactions and with a lower value per transaction The Individual consumer's privacy argument wiII be considerably stronger with respect to digital money transactions, and the volume of digital money transactions likely to be so large as to present a forbidding technological problem for meaningful law enforcement analysis.

It is still highly uncertain what particular impacts digital money will have on money laundering and law enforcement. The technology of digital money is neither mature nor stable, What is certain is that schemes for digital money will make it easier and faster to transfer payments over electronic networks and wiII open new possibilities for both anonymity and record keeping It is vital to consider the impact of digital money when examining approaches to using wire transfers to detect money laundering. This may Involve extending existing requirements to cover digital money, or it may involve specifically excluding digital money so that new requirements do not Inadvertently cover this new technology

[4] David Chaum, personal communication, Columbia University Seminar on Digital Cash and Electronic Money, April 21, 1995

SOURCE Off Ice of Technology Assessment, 1995

gally hold money offshore for a number of reasons, adding to the difficulty of recognizing money launderers (see chapters 1 and 5 for more on this point). Some financiers argue that subjecting wire transfer records in the United States to routine law enforcement scrutiny could increase the tendency of corporations to hold money offshore, or cause the development of competing offshore netting mechanisms, thereby eroding profit centers for U.S. banks, reducing tax revenues, and exacerbating the problems of law enforcement. This may not be a strong likelihood, but the risk tends to undercut the acceptability of wire transfer monitoring to the U.S. banking industry and to corporate money managers.

Separate from bank secrecy laws, most European countries have data protection laws that allow or require the government to prohibit personal

data generated within that country from being transmitted to a country with inadequate privacy laws.[12] These data protection laws are encouraged or required by the Organisation for Economic Corporation and Development's (OECD) Guidelines and a Council of Europe convention. The European Union (EU) also is finalizing a data protection directive that requires all member states to harmonize standards of data privacy. As drafted, the EU Data Protection Directive on data protection requires member states to bar the export of data to a country with inadequate protection standards unless the customer explicitly consents and desires the transfer to take place. It should be noted that the EU Data Protection Directive provides exemptions for law enforcement gathering and processing of data, a limited recognition of the fact that data protection standards do not dovetail with law enforcement's mission and needs. Should Congress decide to implement some form of wire transfer monitoring, tensions with the EU may be averted by negotiations intended to result in an EU pronouncement that its data protection principles are not meant to impede the detection of money laundering in international wire transfers.[13]

## TECHNOLOGICAL CONFIGURATIONS

The MITRE Corporation, in the course of work for federal drug control agencies, developed a proposal for bringing information technology to bear on the problem of electronic money laundering. Although sketchy in particulars, this proposal aroused congressional interest that led to the request for this OTA assessment. This concept, with some necessary detailing, was used as the basis for the first configuration presented below, which is rejected as impractical.[14] More recent versions of MITRE's proposal depart from that model.[15]

Alternative combinations or configurations of technologies for monitoring wire transfer data, as developed by OTA applying technologies discussed in chapter 4, vary along several axes (see table 7-1), including:

- the purpose or appropriate use of the proposed system;
- the site or institutional location of the monitoring system—banks, wire transfer system facilities, a law enforcement agency, or FinCEN;
- the kinds of data used, including additional data to be matched with funds transfer data; and
- the degree to which certain kinds of transfers would be reported or automatically exempted from reporting.

The possible location of a monitoring system is a particularly important consideration. Each location would provide access to different data. *Banks* have data on the wire transfers that they originate, receive, or transmit, as well as data on customer accounts and information gleaned from "know-your-customer" policies. Many wires passing through money center banks may not relate to a customer account, however, because the bank is merely serving as a conduit for another bank.

---

[12] Personal data includes any information relating to an identified or identifiable individual.

[13] U.S. corporations have already lost remote data processing business due to the European perception that the United States does not adequately protect data (see chapter 6). Negotiations with the EU. over wire transfer monitoring would provide an opportunity to clarify the EU's stance towards the data processing and transborder flow of information issue.

[14] For example, the system would look for markers or indicators, such as code words like "Butterfly" used as the name of the transfer originator, or round dollar transfers (e.g. $5 million dollars). When OTA discussed these indicators with bankers, however, we learned that some of the indicators (including round dollar transfers) were or resulted from common business practices. For example, most foreign exchange trades are in round dollar amounts.

[15] Various versions of the MITRE proposals appear in Jim Dear, "Toward a National Architecture for Detecting Money Laundering," Unpublished MITRE Technical Report, December 1991; DEA Strategic Information Resource Management Plan, Office of National Drug Control Policy, March 1992; Jim Dear et al, "Development of an Automated Wire Transfer Analysis System," Unpublished MITRE White Paper, April 1992.

TABLE 7-1: Technological Configurations

| | 1. Automated Informant | 2. Computer-Assisted Examination by Bank Regulators | 3. Targeted access to Records for FinCEN | 4. Two-Level Screening and Evaluation |
|---|---|---|---|---|
| **Purpose** | Detection of new suspects or illicit activities | Detection of new suspects or illicit activities | Support for already initiated investigations and prosecutions | Both detection and support for ongoing investigations and prosecutions |
| **Technology** | Knowledge-based system; uses knowledge-acquisition, data analysis, knowledge-sharing, | Knowledge-based system with supplementary data-analysis tools | Requires copying and forwarding systems, otherwise builds on FinCEN's existing AI system | Requires copying and forwarding systems, otherwise builds on FinCEN's existing AI system |
| **Site(s)** | Uncertain. Could be at banks, wire transfer systems, law enforcement agencies | Banks-either all with access to Fedwire or CHIPS, or all money-center banks | FinCEN | Money center banks and FinCEN |
| **Data** | Wire transfer messages; immediate copies | Bank records: wire transfer records, account records | Specific (requested) wire transfer records; many govt. and commercial databases | Wire transfer records not exempted by banks under guidelines; many govt. and commercial databases |
| **Exemptions** | None | None | All wire transfer records unrelated to already suspect accounts or individuals | Most wire transfer records, according to guidelines to be developed |
| **costs** | High | High for banks and for govt. | Moderate for govt., moderate to low for banks | Moderate to low for banks; high for govt. |
| **Limitations** | Probably impossible now because of lack of useful profiles; unacceptably high number of false positives, etc. Serious privacy issues | Imposes new law enforcement role on bank examiners. Conflict between technological capacity needs and portability,<br>May be impossible now because of lack of useful profiles | Serious policy issues, Requires legislation granting administrative "electronic subpoena" with detailed safeguards | Severe privacy issues, but can be partially alleviated by safeguards |
| **Evaluation by OTA** | Rejected | Rejected | Potentially effective; merits prototyping | Greatest potential enhancement of law enforcement intelligence capability; merits prototyping |

SOURCE: Office of Technology Assessment, 1995.

For CHIPS, monitoring could be done (or targeted access provided) at the 35 to 40 U.S. participating banks, all in New York; most of the wire transfers pass through the 10 or 12 largest commercial banks. Fedwire connects about 11,700 depository institutions; it would probably be most efficient to do any screening, monitoring, or record retrieval at the 12 Regional Federal Reserve Banks. Most Fedwire transfers that involve international transactions go through the New York Regional Bank. SWIFT transfer instructions are used by about 148 U.S. banks and 300 U.S. sub-

sidiaries of foreign banks.[16] Perhaps three-quarters of these transfer messages too are believed to go through a dozen very large banks.

If money launderers became aware that transfers through these banks were monitored, they might seek to move their funds through other banks. However, smaller banks not now having access to CHIPS or SWIFT probably would be deterred by the costs from joining these systems to serve a relatively few customers. CHIPS participation requires at a minimum having a New York office, plus approval by Clearing House bank members. SWIFT participation costs include a membership fee of $20,000 to $30,000 annually, and interface equipment costing from $20,000 to $100,000.

The additional compliance cost burden on banks would probably hurt least those banks with the highest volume of transfer traffic and bear most heavily on those with relatively low volume. Assuming those costs would be passed on to customers, the most likely result would be to further concentrate wire transfer traffic in a few very large money center banks.

Wire transfer systems keep electronic copies of all of the transfers passing through their networks (although in the case of SWIFT, the information not essential to routing the wire transfer is encrypted and not readable by the central computer). It is important to note, however, that there is no single centralized database of wire transfer records to be mined. For records earlier than 1994, there were 14 wire transfer systems to be considered (SWIFT, CHIPS, and Fedwire, the latter dispersed among the 12 regional Federal Reserve Banks). By the end of 1995, Fedwire records will be aggregated in only two locations, and eventually will be consolidated at one location. Fedwire records are kept on line for three days, on tape for six months, and on microfiche for seven years.

Regulatory authority over these systems differs: Fedwire is government operated, but CHIPS is owned by a consortium of banks and SWIFT is a foreign corporation which has a North American operations office in New York. CHIPS is effectively unregulated now, although subject to state regulatory authority. Imposing federal monitoring obligations on this institution would be breaking new ground. The same is true of SWIFT. Also, as pointed out in chapter 2, SWIFT transfers are encrypted throughout their passage from bank to correspondent bank, which would greatly complicate screening.

FinCEN has access not only to financial reports required by federal law (e.g., Currency Transaction Reports), but also to many other law enforcement and commercial databases to support investigations of money laundering. Other federal agencies lack FinCEN's data access, as well as the expertise in artificial intelligence (AI) methods and the building of law enforcement detection systems. This is why FinCEN is given special attention as a logical location for analyzing wire transfers.

Beyond the technological considerations, the site chosen for the monitoring system can have large ramifications in terms of costs and who bears the costs. The costs of systems development, deployment, operation, maintenance and updating, and personnel training may differ by location, and decisions will have to be made about the extent to which these costs are covered by government or imposed on financial institutions. Throughout this analysis, there has been concern for the burden that might be placed on private sector industry and institutions, especially banks.[17] The potential burden on the banking industry, however, must be weighed in the context of the obligations that U.S. taxpayers and the U.S. government assume on be-

[16] In addition, there are about 55 other nonbank financial institutions that use SWIFT, such as brokerage houses. As more emphasis is placed on Bank Secrecy Act (BSA) compliance by nonbank financial institutions, monitoring might be extended to these wire transfer users.

[17] The Supreme Court has observed that imposition of costs through recordkeeping requirements do not deprive banks of due process of law; see, for example *California Bankers Ass'n v. Schultz,* 416 U.S. 21 (1974).

half of banks—e.g., the recent salvaging of failed and failing banks and savings-and-loan institutions, the total cost of which has been estimated at between $175 billion and $500 billion. None of the configurations discussed below create a bottleneck that could impede the speed, efficiency, and security of wire transfers.

The location of the screening systems will also affect privacy and confidentiality. *Each of the two alternatives presented as feasible would require some modification or amendment of existing privacy laws;* the necessary modifications are spelled out in detail for each option below.

## OPTIONS

Five options, based on four technological configurations, are briefly set out below:

*Option 1:* An automated informant (this is the closest to the MITRE proposals mentioned above).

*Option 2:* Computer-assisted examination of wire transfer records by bank regulators.

*Option 3:* Targeted access to wire transfer records for FinCEN via subpoena.

*Option 4:* Two-level screening and evaluation.

*Option 5:* Incremental deployment of wire transfer screening (i.e., a progression from option 3 to a combination of options 3 and 4).

The first two options, after full assessment, appear to involve severe problems that almost certainly outweigh the potential benefits of their implementation. Options 3 and 4 are much more promising, because they build on systems already in place, as well as take advantage of the new Treasury regulations on wire transfer recordkeeping (see figures 7-2 through 7-5). Technical problems common to all five options, as discussed above, are as follows:

- The number of money laundering transactions constitutes a relatively small proportion of all wire transfers.
- Only small amounts of information are contained in a wire funds transfer message.
- It is difficult to characterize or describe a "typical" money laundering transaction or a "typical" illicit wire transfer.
- The many ways of cleaning or hiding money would require the use of many different profiles of money laundering,
- Money laundering transactions often resemble ordinary business activity.

### Option 1: An Automated Informant

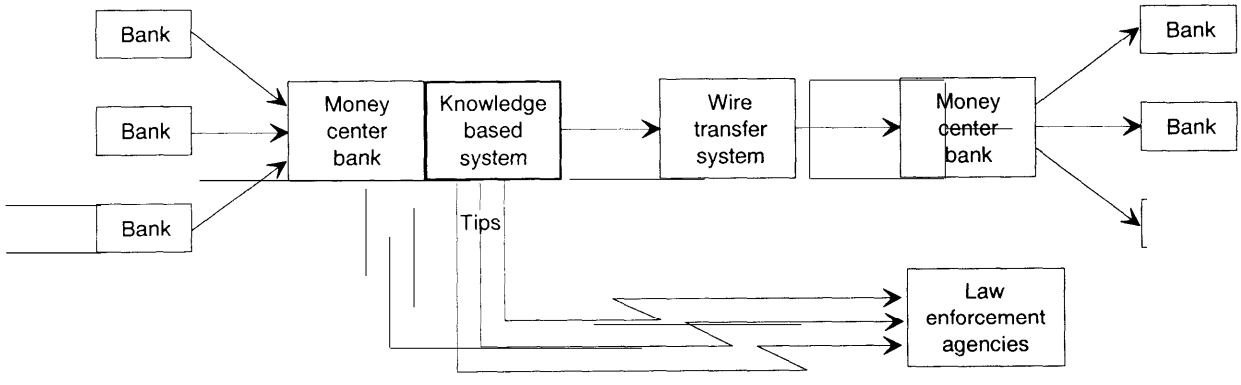
An AI-based system would monitor all wire transfer traffic, comparing messages to profiles, or characterizations, of illicit transfers. The AI-based system would "recognize" some transfer messages as suspicious (i.e., matching the profile) and tag them for inspection by law enforcement analysts. This configuration would be designed to generate new leads for investigators. It would not search for specific individuals or organizations, even those already suspect, and thus would not be used to support already initiated investigations. The system would be fully automated, analyzing copies of messages almost as soon as the original was transmitted.

This would be a *knowledge-based system.*[18] Standard *knowledge-acquisition* and possibly *data-analysis techniques* might be required to construct the knowledge base. Rudimentary *knowledge-sharing technologies* might be important for maintenance and updates of profiles. Secure data transmission and storage are important.

When this concept was originally suggested for OTA assessment, it was unclear where such a system would be located: at three wire transfer systems, at 10 to 20 major money center banks, or at one or more federal agencies. The first two choices would impose burdens on private sector

[18] Please see chapter 4 for explanation of the italicized technical terms.

Figure 7-2: Automated Informant




SOURCE Off Ice of Technology Assessment, 1995

organizations, particularly banks. Multiple systems at banks or wire transfer facilities also would have to conform to different systems of recording and retrieving records at each place. The latter choice would require copying, transmission, storage, and maintenance of records within government, creating a new database.

This configuration is fatally flawed, because there is insufficient information on which to base the profiles required for this system. Even if profiles could be generated, the information carried on a wire transfer alone is insufficient to permit matching to any profile of enough complexity to be useful. If these obstacles could be partially overcome, there would at best be an extremely high proportion of false positives. The need for frequent updating of profiles would be a continuing problem, especially if the system were distributed among a number of banks. In any location, but especially banks, it would be necessary to make sure that profiles did not fall into the hands of money launderers, because the profiles would be a reliable guide to avoiding suspicion by law enforcement agencies.

Costs would be high for development of a system capable of handling the volume of traffic necessary, and flexible enough to interface with multiple institutional systems. Maintenance costs would be high because of frequent updating. Who bears the costs could vary according to location; all locations would impose at least some costs on financial institutions.

Intrusion on privacy would be a serious problem at all locations. [19] The issue of secondary use of financial data (i.e., use for purposes other than that for which the data were obtained) would arise at all locations, including banks. Problems of ensuring data security and objections to unfounded investigations of false positives would also arise at all locations. At FinCEN, an additional issue would arise-creation of a new government database. Modification of the Electronic Communications Privacy Act (ECPA) would be needed to provide law enforcement with full access to wire transfers. At the same time, to minimize the intrusion, the authorizing legislation would need to spell out the precise purpose to which data maybe

[19] This is not to suggest that financial confidentiality is absolute today: banks monitor traffic for other reasons, such as foreign asset control. Banks are required to refuse to execute unauthorized transfers out of certain accounts held in this country by nationals of certain hostile or suspect countries (e.g., Libya, Iraq) with whom it is illegal to do business. This regulation is administered by the Office of Foreign Asset Control in the Department of the Treasury. See chapter 4 for a technical discussion of the system.

put, to forbid other uses of data, to limit storage of data, and to provide safe harbor for banks against customer suits.[20]

***Evaluation:*** *This option was rejected as technically difficult, probably impossible in the immediate future because of difficulties of profiling; likely to have poor operating characteristics (excessive false positives); carrying high monetary costs; and being broadly and indiscriminately intrusive into individual privacy and corporate confidentiality.*

## Option 2: Computer-Assisted Examination of Wire Transfer Records by Bank Regulators

Bank examiners,[21] using AI-based systems, would examine all wire transfers at all banks in the course of regular or continuing bank examinations.[22] The examiners would use government-owned hardware and software, which would automatically compare transfer records to profiles developed by law enforcement experts. The equipment would necessarily be portable in all but the largest banks.

Wire transfers identified as suspicious would be transmitted to one or more law enforcement agencies for investigation. The primary product of this system would be identification of new suspects, i.e., generation of leads. Subsidiary software might however allow examiners to search for additional records related to already identified suspects, and possibly allow them to relate "know-your-customer" information to the records they identify as suspect.

This would be a *knowledge-based system*. To supplement the automated scan, analysts would need *data-analysis software*, possibly including *visualization* and statistical tools.

Lack of knowledge for generating profiles is a virtually insurmountable obstacle to this option, as well as to option 1. In addition, patterns of money laundering activity involving several banks would probably not be detected. Because bank examinations in most cases are scheduled and not continuing, this configuration (in all but the largest banks) would require examination of records accumulated over periods of months. The system would require banks to make changes in their recordkeeping and retrieval technology, at substantial costs, in order to interface with the examiners' system. However, security would not be a major problem because the data would remain within banks. These changes would likely be least burdensome for the money center banks.

Bank examiners regard themselves as supervisors, not investigators. Although the Money Laundering Suppression Act of 1994 has already expanded the responsibility of bank regulators, this configuration would fundamentally change their role, giving the regulators de facto new law enforcement functions far beyond their current "safety and soundness" mission. The number of examiners would probably have to be expanded, and a significant amount of new training would be required.

Costs would be high for technology development and maintenance in this configuration. Development would be a significant challenge given the needs for capacity, portability, and multiple interfaces. Standardization of data would be required far beyond what the new regulations require. Primary costs would be borne by government, but banks could incur significant costs for adapting their record storage and retrieval systems.

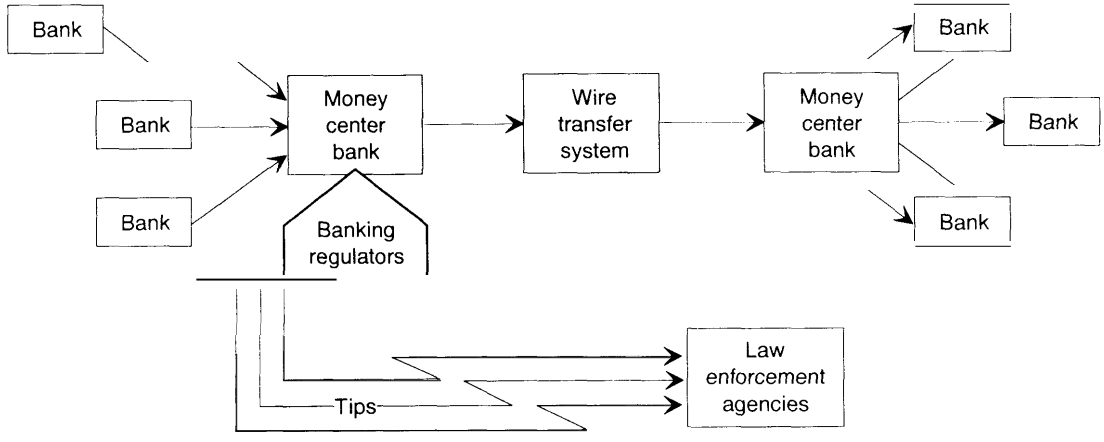
---

[20] "Safe harbor" is legislative protection against being sued, in this case by customers for violations of privacy.

[21] The Office of the Comptroller of the Currency for federally chartered banks, the Federal Reserve System for most state-chartered and foreign-owned banks, the Federal Deposit Insurance Corporation for state-chartered banks not members of the Federal Reserve System.

[22] Bank examinations, now concerned primarily with the safety and soundness of the banks, are often as much as two years apart. However, in very large money center banks such as those that handle nearly all international wire transfers, bank examiners are usually continuously on premises.

Figure 7-3: Periodic Examination by Banking Regulators




SOURCE: Office of Technology Assessment, 1995

Banking regulators already have access to customer records, but further privacy concerns again include secondary use of financial data for law enforcement investigation, potential creation of a new government database, unfounded investigation of false positives, and problems of data security. Bank regulators are exempt from the Right to Financial Privacy Act (RFPA); but they may need an express waiver to permit them to access stored wire transfers. ECPA would have to be amended to provide an exemption for banks disclosure and reporting to law enforcement agencies.

*Evaluation: This option is rejected as technically difficult, institutionally disruptive (e.g., it entails a fundamental change in role of regulators), heavily intrusive, and likely to be ineffective because of lack of profiles, sparseness of data, limited scope, and lack of timeliness. It would be costly to both government and the banking industry.*

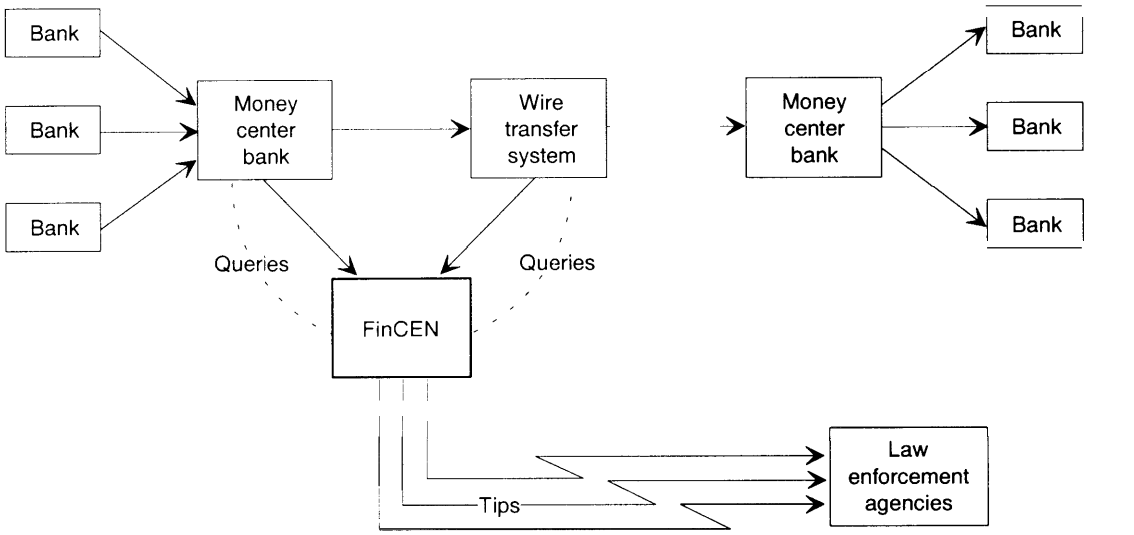
## Option 3: Targeted Access to Wire Transfers for FinCEN

Banks and wire transfer systems would be required to provide wire transfer records electronically to FinCEN in response to its specific requests, provided the data requested are from a limited period (e.g., not over two years old). FinCEN would hold legislatively conferred subpoena power to make such requests on the basis of documented suspicion derived from a conflux of Currency Transaction Reports (CTRs) selected by its existing AI system, law enforcement tips, and link analysis. This configuration would have a built-in procedural check on the exercise of law enforcement power: the grounds for such suspicion would be challengeable in court during a prosecution resulting from such an inquiry. In some cases, a request for transfers associated with a suspect name or account number would have to be issued to many banks, but the number of relevant wire transfers would still be limited because the subject, or target, is singular.

The wire transfer information would be analyzed in the context of other government and commercial data bases, through link analysis. Use of this system would primarily confirm and sharpen leads already generated and provide support to law enforcement investigations and prosecutions. Few new leads would be generated by its use. FinCEN would have authority to store and maintain data, once received, for a limited period of time. Normally, subpoenas require the timely return of records.

Building on an already existing AI system at FinCEN, this new system would target wire transfer records to be requested. The selection would be based not on information carried on the wire trans-

Figure 7-4: Targeted Access




SOURCE: Office of Technology Assessment, 1995

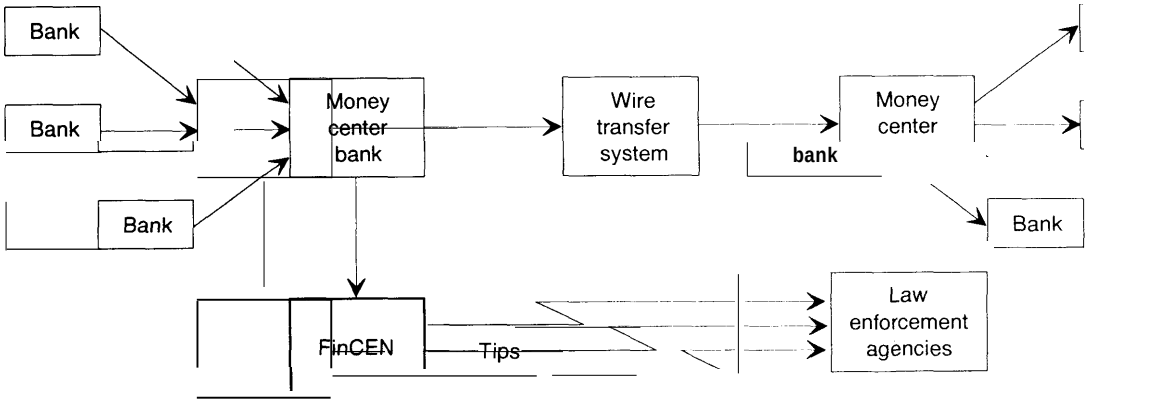
fer but on other grounds, already established. Thus, it would be able to reduce enormously the number of wire transfers to be examined. A reasonably small number of false positives should result, in comparison with those that would be generated by option 1. The system would allow FinCEN to be more responsive to local and state enforcement agencies attempting to track funds moving outside of their own jurisdictions.

This configuration most closely approximates current law enforcement practice. As a consequence, it is likely to be least objectionable to privacy advocates. Nevertheless, as indicated in box 7-2 it would require a nearly novel "administrative" subpoena power for a law enforcement agency, a departure from the traditional model of criminal subpoena issued by a grand jury, setting a potentially broad precedent. Moreover, an "electronic subpoena" direct from FinCEN to the banks would streamline the subpoena process and facilitate timely investigations. Careful sculpting of the criteria for issuing this subpoena may be able to insulate it from constitutional attack, but parties would likely have no opportunity to quash the subpoena. Nonetheless, even civil libertarians and privacy advocates may prefer it to other options.

Costs should be moderate for government and for banks, compared to costs for option 1. This system would build on systems already in place for money center banks, which must already have retrievable records (most on optical disks). FinCEN's existing basic systems are utilized but new capacity will be required to store and analyze an increased number of records.

*Evaluation: This option has the promise of providing usable support to law enforcement at the operational/field level, in a way not disruptive of current law enforcement habits and culture, at moderate cost. It would require a new and fundamentally different legislative mandate of power to an executive agency ("electronic subpoena" ) to which privacy advocates are likely to object. It would however have an additional benefit of gradually generating much needed knowledge of the way wire transfers are used in money laundering and the patterns of behavior that indicate illicit transfers+". e., it could over time contribute to the creation of the "profiles" that are now lacking.*

Figure 7-5: Two-Level Screening and Analysis




SOURCE: Office of Technology Assessment, 1995

## Option 4: Two-Level Screening and Evaluation

Banks and/or wire transfer systems would operate one level of screening of wire transfer traffic, using guidelines developed by the Department of Treasury/FinCEN in consultation with banks. AI-based systems adapted to interface with the banks' own record keeping and retrieval systems would be employed. Banks would not select suspicious records per se (avoiding the problems of profiling and of sparse message data). Instead, they would eliminate "nonsuspicious" transfers+. g., those originated by established and well-regulated banks, national and international corporations, and well-known customers.

The remaining, greatly reduced traffic-possibly about 25 percent of the total, or 150,000 transfers per day, which is still an enormous increase in FinCEN's workload—would be copied and sent to FinCEN where they would be further filtered by an AI system[23] to identify suspect subjects and accounts. The suspect records would then be analyzed by FinCEN's link analysis operations (i.e., matched with data from CTRs and from government and commercial databases for contextual information).

The primary product here would be new leads. Evidentiary support for ongoing investigations might also be generated. The system might not catch multibank laundering operations if differences in banks' implementation resulted in different levels of screening.

Costs would be moderate to high for banks and high for government. The system would require a substantial increase in technology for banks to screen transfers. Bank systems could build on existing Office of Foreign Assets Control systems (see box 4-2), but these are far less complex. Processing of 150,000 records daily at FinCEN would require major new capacity and human resources; this would be an order of magnitude increase in current workload in spite of the huge reduction in volume of transmissions monitored.

Privacy concerns are severe; they are almost the same as those discussed under option 1, although here they are better balanced by expectation of significant benefits. It is likely that individuals and closely held corporations would be least likely to be exempted; hence those with the strongest privacy interests would suffer the greatest intrusion. In this option, much "nonsuspect" data will not leave the bank, and false positives should be

[23] See option 5, the option 4 AI system may use profiles developed through experience with option 3 if a phased approach has been adopted.

somewhat fewer than in option 1. This is still secondary use of financial data for law enforcement investigation; it would create a new government database, and result in some unfounded investigations of false positives. There are problems of data security, and there is large-scale computer matching of commercial and law enforcement databases. To partly offset these drawbacks, the existence and extent of monitoring and analysis should be made public. Treasury guidelines should be expressly authorized by statute, which should clearly spell out criteria. The existing safe harbor provision for banks in RFPA should be broadened to include wire transfers in electronic storage. ECPA and RFPA should be amended to clarify that the reported wires may be used in evidence without tainting investigations or exposing the government or banks to civil suit. Security will be important at banks, at FinCEN, and in transmission from one to the other.

***Evaluation***: *This option is most likely to have high payoff for law enforcement. It is capable of incremental improvement; with experience, the Treasury guidelines and the knowledge-based systems used at FinCEN should become much more effective. Costs are potentially high but may be balanced by increased asset seizure. Privacy concerns are strong; the question is whether detailed legislation and watchful congressional oversight could make them acceptable.*

## Option 5: Incremental Deployment of Wire Transfer Screening

All efforts to control electronic money laundering would greatly benefit from thorough research into how, why, and by whom legitimate wire transfers are used. Surprisingly little is known about this subject. This is largely because wire transfer data have been both legally protected and practically difficult to access. It should be possible, however, to "sanitize" a body of wire transfer data (that is, strip off or disguise identification with specific persons or organizations) in somewhat the same way that census data is sanitized for demographic and sociological research. Increased understanding of legitimate usage of wire transfers, along with the patterns of commercial behavior that it represents, might contribute significantly to the ability to recognize illicit transfers by their deviation from such patterns. If no significant differences appear, as many experts believe will happen, this will provide further insight into the potential practicality of proposed strategies for screening wire transfer data, including those laid out above.

Abuse of wire transfer systems for illicit purposes effectively undercuts law enforcement goals for controlling drug trafficking, dismantling criminal organizations, attacking terrorism, and reducing white collar crime and fraud. *If Congress is convinced that this problem requires efforts to strengthen the hand of law enforcement, even at the cost of exceptions to existing privacy protections, a phased introduction of advanced information technology, including the use of artificial intelligence techniques, should be considered.*

Such a program might begin with prototyping of option 3, which emphasizes targeted access to wire transfers for FinCEN. Option 3 is the lowest cost configuration, places the least burden on banks (giving them a reactive rather than proactive role), and probably allows the most adequate safeguards for privacy and corporate confidentiality, while significantly increasing the usefulness of wire transfer records for law enforcement and the amount of support that FinCEN and the banking industry can provide state and local as well as federal law enforcement.

Experience with option 3 at both the prototyping and implementation stages should contribute significantly to knowledge about how criminals and criminal organizations use wire transfers and perform money laundering.

Option 3 cannot completely solve the international money laundering problem; even if highly successful, it will support investigations or prosecutions already initiated rather than identifying new suspects or generating new leads. It may therefore be deemed necessary later to implement option 4 as well as or to replace option 3. If so, the earlier steps will have provided a foundation of improved information about money laundering operations and about both licit and illicit use of

## BOX 7-4: Comments of FinCEN on Technological Options

Options 4 and 5 would give FinCEN significant new responsibilities and new powers Once OTA had conceptualized these approaches, therefore, it was appropriate to ask FinCEN managers whether they would view these options as effective enhancements of their capabilities to support law enforcement agencies,

With regard to option 3, targeted access to wire transfers for FinCEN, Director Stanley Morns says that "this system [would] pose tremendous tactical value to FinCEN and the law community as a whole."[1] Director Morris explained that FinCEN IS often asked by federal, state, or local Investigators to search for any wire transfer activity related to a suspect The law enforcement officers are often reluctant to subpoena bank records because the bank might inform its customers, might be conservative in the records it would reveal, might be located overseas, or might even be in complicity with suspects FinCEN currently does not have the capability of conducting such searches for Investigators "Accordingly, " Mr. Morris said, "giving FinCEN analysts the ability to enhance leads by querying specific banks to obtain records of wire transfers Involving particular suspect accounts or individuals would be of tremendous value to law enforcement efforts in piecing together the trails of highly complicated money laundering schemes. " While acknowledging that privacy concerns would arise, Mr. Morris said that "it appears that a strictly tailored system could be employed to ensure that wire transfers are only obtained from a bank pursuant to a reasonable suspicion (i.e., they seem to relate directly to and are essential to a pending money laundering investigation) "

Mr. Morris noted, nonetheless, that option 3 is "purely tactical" and would not lead to new detection or identification of new suspects. He commented that "from the intelligence analyst's perspective " this option should ideally coexist with one of the others, preferably option 4, in other words the progression envisioned as option 5 above.

Option 4, in Mr. Morris's view, "offers the greatest advantages in providing intelligence analysts with the comprehensive data and tools they need to accurately identify suspect wire transfer activity patterns and eventually build the capability to detect suspect wire transfer transactions " Mr. Morris noted that a series of measures could be undertaken to reduce the amount of data that would be transferred to FinCEN to a manageable volume, and that these measures need not "burden the banks with a detection task. " Because this option would allow analysts to "piece together complete paper trails and [detect] emerging/shifting patterns," it would offer "outstanding analytical advantages, " and at the same time create a learning process to help analysts in the future distinguish legitimate from illicit activities

Taken together, Mr. Morris concluded, these options would "make our efforts more productive and goals easier to achieve. "

[1] Quotations in this section are taken, with permission of FinCEN Director Stanley Morris from a letter he sent to Vary Coates, OTA project director, on April 24, 1995, in response to her request that he review draft descriptions of the options proposed in this chapter These descriptions were prepared before the chapter was written, and some details of the options were subsequently modified or clarified as the team and its advisors reworked the descriptions. Option 5 was created after the material reviewed by Mr. Morris but before his letter was received. In all fundamental ways, however, the first four options are consistent with the material reviewed by Mr. Morris and others at FinCEN.

SOURCE: Office of Technology Assessment, 1995

wire transfers. The support provided for investigations and prosecutions by option 3 may have resulted in seizure of illegal assets sufficient to offset much of the cost of systems development for both options 3 and 4. If attention to security and privacy have been meticulous, Congressional and public trust may act to reduce resistance to implementation of option 4. These factors would en-

courage implementation of option 4 in the hope of further tightening the noose on electronic money laundering.

On the other hand, it could become apparent that because of the success of option 3, large scale money laundering has tended to move away from use of wire transfers and toward other modes of moving money—possibly the use of new forms of payment such as digital money. In this case, it may be sufficient to maintain option 3 as a continuing deterrence, without the additional investment necessary for option 4.

## Additional Considerations

The technological options presented above would be significant innovations in law enforcement strategies for control of electronic money laundering (see box 7-4). The options recommended for prototyping call for changes in legislation, institutional missions and procedures, and privacy protection policies, as well as for investment in technology. These steps are perhaps best approached as experiments in public administration, with recognition that their direct costs, degrees of effectiveness, and potential secondary impacts—social benefits and costs—are not fully predictable. If Congress chooses to authorize one or several of these options, it may also want to set up special oversight arrangements to be sure that each successive phase of implementation is effective and beneficial before the next phase is undertaken. Oversight arrangements would be particularly important because money launderers, and criminal organizations in general, appear to be flexible and adaptable in devising ways to counter law enforcement initiatives and technological advances.

The coming development of digital money (see box 7-3), especially in connection with the Internet and the "National Information Infrastructure," is one example of a technological trend or future uncertainty that could have a strong impact on the effectiveness of these or other strategies for control of electronic money laundering. A watchful eye on this electronic money, as it develops, could prevent investment in wire transfer screening technology that might thereby be rendered less effective, or it could permit timely adjustments to the screening technology and to the laws and regulations that structure its use, so as to maintain and enhance its effectiveness for the foreseeable future.