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

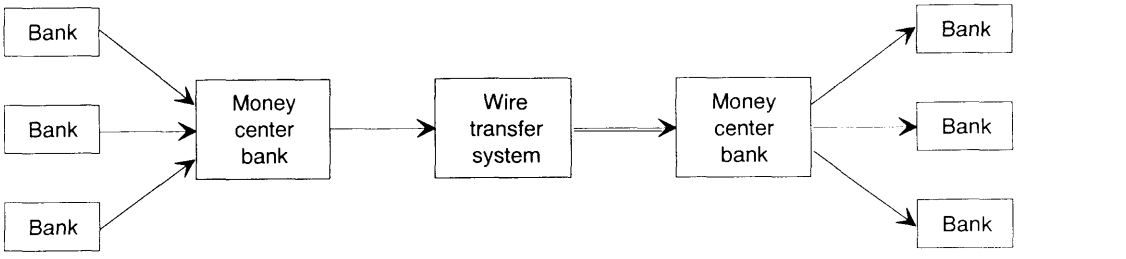
are easily hidden. Their audit trails are obscured within enormous databases that are generally safe from law enforcement investigators. By comparison, physically smuggling cash and even paper-based monetary instruments across national boundaries—although often successful—is slow and unacceptably risky.

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, 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

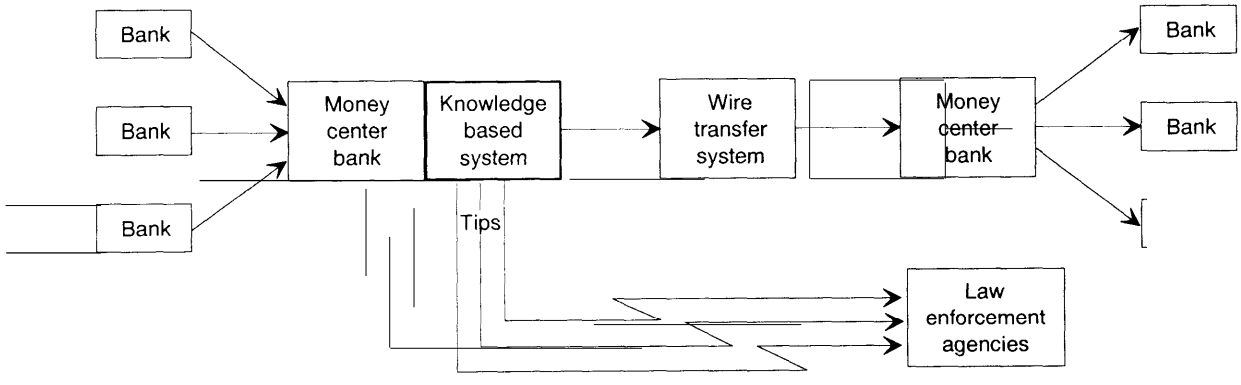
An AI-based system would monitor all wire transfer traffic, comparing messages to profiles, or characterizations, of illicit transfers. The AI-based system would "recognize" some transfer messages as suspicious (i.e., matching the profile) and tag them for inspection by law enforcement analysts. This 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.

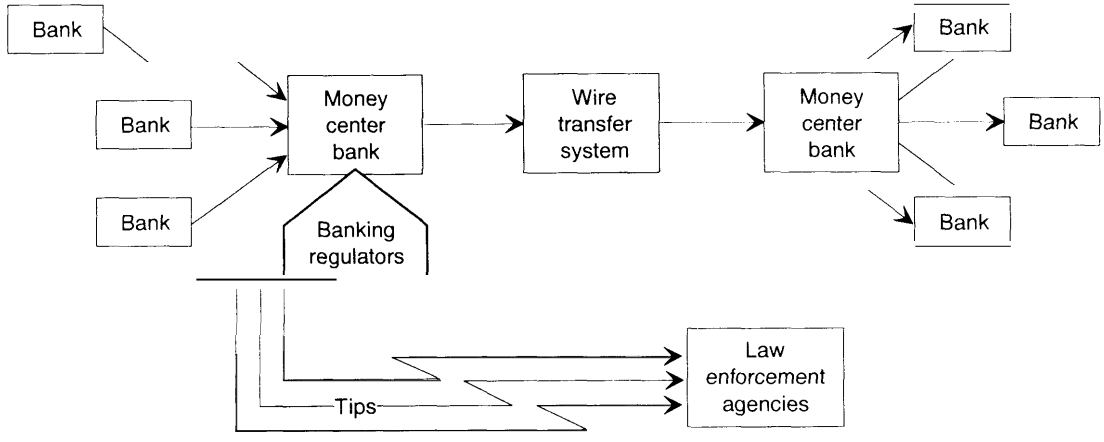
---

[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.

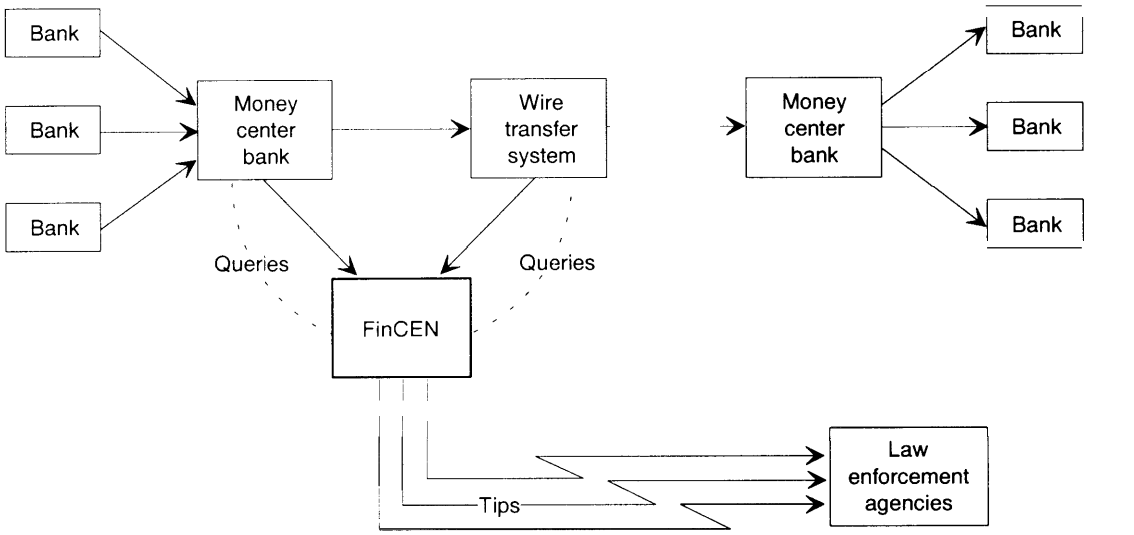
Option 3: Targeted Access to Wire Transfers for FinCEN

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

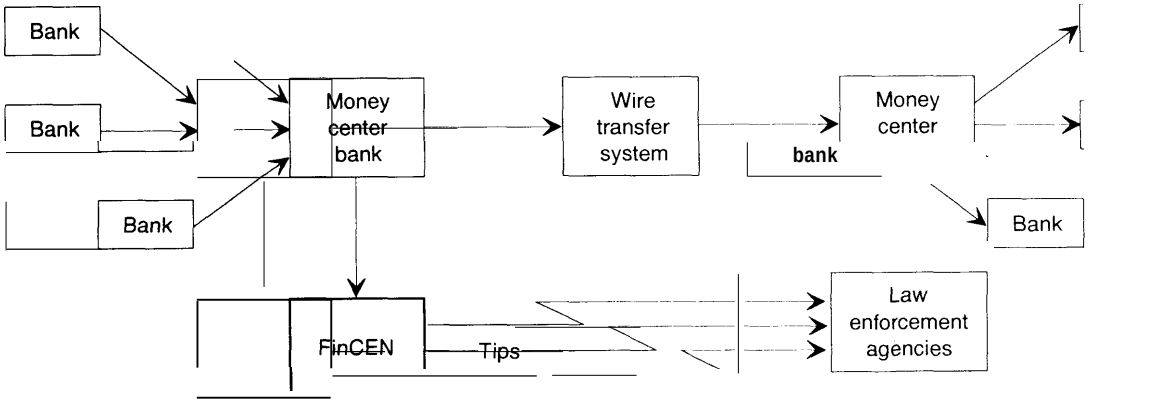
fer but on other grounds, already established. Thus, it would be able to reduce enormously the number of wire transfers to be examined. A reasonably small number of false positives should result, in comparison with those that would be generated by option 1. The system would allow FinCEN to be more responsive 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.