Money Laundering and Law Enforcement 3

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

LAWS AND REGULATIONS

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

SOURCE: Office of Technology Assessment, 1995.

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

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

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

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

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

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

covering the licensing of nonbank money transmitters.

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

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

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

---

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

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

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

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

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

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

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

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

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

FEDERAL AGENCIES' ROLES AND RESPONSIBILITIES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

SOURCE: Office of Technology Assessment, 1995.

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

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

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

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

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

STATE LAW ENFORCEMENT

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

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

---

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

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

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

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

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

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

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

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

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

THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN)

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

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

FinCEN analysts and agents support law enforcement in several ways:

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

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

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

---

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

[33] As of January 1995.

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

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

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

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

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

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

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

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

BOX 3-1: Databases Used by FinCEN

Government Databases:

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

Commercial Databases:

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

SUMMARY

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

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

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

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

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