THE LOW DOWN ON DIRTY MONEY

BY RICHARD HOROWITZ

IN 1992, a North Carolina resident was convicted of money laundering for having received a cash payment of $60,000 from a drug dealer. The resident, who accepted the money wrapped in small bundles and delivered in a brown paper bag, had no involvement in the drug underworld, organized crime, or terrorism. Nor did she have a criminal record. The defendant was a local real estate agent who had accepted the cash as partial payment on the sale of a home.

THE NORTH CAROLINA conviction was upheld on appeal because, according to the law, knowingly accepting proceeds of illegal activity is prosecutable as money laundering. The court held that the defendant must have realized that the origin of the cash was drug related based on the other party's "flashy lifestyle" and his method of conducting business. The case illustrates how "willful blindness" or "deliberate ignorance" can be considered knowledge and leave an individual or corporation vulnerable to legal action.

Banks and other legitimate commercial businesses are targeted by money launderers, because money laundering—by its very nature—requires the participation of a legal enterprise. The proceeds of illegal activities are "laundered" through a legal operation to conceal their true source. Falling prey to these money laundering schemes can expose any commercial enterprise to legal liability if the court determines that the business failed to recognize suspicious activity or, worse, ignored warning signs.

Estimates put the money laundering problem at $300 billion to $500 billion a year. The U.S. Department of State has twenty-one nations on its 1997 High Priority list, which identifies countries where the most action is needed to stem the money laundering problem. Among the countries listed are the United States, the Cayman Islands, Colombia, Germany, Hong Kong, Italy, Mexico, Russia, Singapore, Switzerland, Turkey, the United Kingdom, and Venezuela.

With their personal experience in dealing with suspicious and criminal activity as well as their industry contacts and resources, security professionals can play a significant role in protecting their companies or banks from unwittingly being used by money launderers. To do this effectively, the security manager must understand the laws designed to stop criminal activities and the techniques used to launder money.

HE COURT HELD THAT THE DEFENDANT MUST HAVE REALIZED THAT THE CASH WAS DRUG RELATED BASED ON THE BUYER'S "FLASHY LIFESTYLE."

U.S. LAWS. U.S. efforts to combat money laundering began in earnest in 1970 with efforts to regulate transactions at banks and other financial institutions. By the mid-1980s, federal regulators were imposing requirements on other companies as well.

BSA. The first major effort came with the passage of the Bank Secrecy Act (BSA) in 1970. Amended several times since, the BSA is designed to counter money laundering efforts that begin with a person making large cash deposits. The BSA requires domestic financial institutions—including banks, securities dealers, currency remitters, and other organizations—to file a Currency Transaction Report (CTR) with the U.S. Treasury Department for all currency transactions of more than $10,000. It also requires individuals to file with U.S. Customs a Currency and Monetary Instrument Report (CMIR) when taking sums greater than $10,000 across U.S. borders, and it prohibits the structuring of financial transactions to avoid the reporting requirements.

IRS code. Federal law moved beyond the financial services industry in 1984, when Congress amended the Internal Revenue Code to require anyone engaged in a trade or business to file Form 8300 whenever they receive $10,000 in cash in a single transaction or several related transactions.

MONEY LAUNDERERS USE A BOGUS TRAIL TO GIVE ILLEGAL EARNINGS A LEGAL PEDIGREE.

Illustration by **Stephen Bauer**

MONEY LAUNDERING OCCURS THROUGH BANK DEPOSITS OF CASH-INTENSIVE BUSINESSES SUCH AS CASINOS, RESTAURANTS, AND RETAIL SHOPS.

This legislation was designed to impede launderers who turned to other businesses to launder money as a way to avoid having their transactions reported to the government under the BSA.

By analyzing the information provided in CTRs, CMIRs, and Form 8300, the Treasury Department can identify patterns of suspicious behavior. For example, CTRs that show the same person making numerous deposits in many different banks in a short time period may alert law enforcement to the need for further investigation.

Criminal offense. In 1986, money laundering became a criminal offense with the passage of the Money Laundering Control Act. This legislation makes it illegal for businesses and individuals to knowingly conduct or attempt to conduct a financial transaction using the proceeds of "specified unlawful activity" (SUA) to promote the unlawful activity; engage in tax fraud or evasion; or conceal the nature, location, source, ownership, or control of the proceeds. Among the activities specified by the statute are drug trafficking, tax evasion, fraud, counterfeiting, racketeering, bribery, embezzlement, smuggling, murder, and kidnapping. Both the person who deposits the money and the person who accepts it can be held liable under the law, which carries a maximum penalty of twenty years imprisonment and fines of $500,000 or twice the amount of money laundered, whichever is larger.

Annunzio-Wylie. The Annunzio-Wylie Money Laundering Act of 1992—under which a U.S. bank can lose its charter or license for BSA and money laundering violations—authorizes the secretary of the treasury to require financial institutions to "report any suspicious transaction relevant to a possible violation of law or regulation." This act also contains a "safe harbor" provision, which protects financial institutions from civil liability against their clients for making such reports.

The federal regulations that grew out of this law require banks to file a Suspicious Activity Report (SAR) on suspicious activity involving sums greater than $5,000. In April 1996, a standardized form was created that must be sent to the Financial Crimes Enforcement Network (FinCEN), a U.S. Treasury Department unit that collects data and provides intelligence on financial crimes to other government agencies. In the six months after the form was introduced, FinCEN reported 31,143 SARs filed, almost half of which related to suspected money laundering or BSA violations. (The remaining reports dealt with crimes other than money laundering, such as embezzlement and check fraud.)

Money remitters. Most recently, in May 1997, the Treasury Department announced proposed regulations under which financial service providers that wire money overseas would have to report to FinCEN suspicious activity and any transfer that involved more than $750. The report would have to include the names of the

sender and recipient of the funds. This regulation specifically targets organizations other than banks that wire money overseas, including small storefronts that can be used in money laundering activities. Like the CTRs and Form 8300, it would give federal authorities another form of documentation with which they could find patterns of suspicious behavior.

Know-your-customer policy. In response to the various money laundering laws and regulations, financial institutions have adopted money laundering compliance programs and know-your-customer (KYC) policies in which they attempt to determine whether a potential customer's business dealings are legitimate.

The depth and scope of a KYC policy depends on the bank and the customer seeking to open an account. At the very least, financial institutions ask customers for proper identification before a new account is opened. For large accounts, however, the institution will likely conduct a more thorough background investigation of the customer.

After years of deliberation, the federal government is expected finally to publish KYC requirements this fall with an effective date in 1998 (although they were not yet out as the magazine went to press).

METHODS. While the only limitation on money laundering schemes is the perpetrator's imagination, all such operations use common tools and techniques. A February 1997 report of the Financial Action Task Force (FATF), an international committee composed of representatives of twenty-six countries, concluded that "no significant new methods of money laundering were identified by [FATF] member states, and indeed a number of traditional money laundering techniques continued to be prominent methods for hiding the proceeds of a crime."

Money laundering schemes generally follow the same overall strategy and method. The first step is for the criminal to place the ill-gotten gains into the stream of legitimate commerce through bank deposits or the purchase of financial instruments or goods. Second, launderers generate a process of "layering" in which the tainted currency is shuffled through a series of shell corporations, wire transfers, bank accounts, and offshore jurisdictions with the intent of obfuscating the original source of funds. The launderers'

AIRING THE DIRTY LAUNDRY

MANY BOOKS, magazines, newsletters, government reports, databases, and Internet sites can help the security manager keep abreast of the latest trends in money laundering.

For an excellent study of money laundering schemes, see *The Money Launderers: Lessons from the Drug Wars—How Billions of Illegal Dollars are Washed through Banks and Business*, by Robert E. Powis, published by Probus Publishing Company, 1992.

For an account of the hidden financial world and an economic analysis of the source of illegal capital, read *The Secret Money Market: Inside the Dark World of Tax Evasion, Financial Fraud, Insider Trading, Money Laundering, and Capital Flight*, by Ingo Walter, published by Harper & Row, 1990.

Also worthwhile is *The Laundrymen: Inside Money Laundering, The World's Third-Largest Business*, by Jeffrey Robinson, published by Arcade Publishing, 1996.

For a cynical view of money laundering, there is "How to Launder Money" in the November 1995 edition of *Liberty* magazine.

A general overview of money laundering and U.S. and international efforts to combat it can be found in *Money Laundering: A Framework for Understanding U.S. Efforts Overseas*, published by the U.S. General Accounting Office, May 1996 (also available on *Security Management Online*).

Security managers can also check *Money Laundering Alert*, a newsletter published in Miami (800/232-3652). The newsletter sponsors a site on the World Wide Web at http://www.moneylaundering.com.

The Financial Action Task Force publishes two reports that can be helpful to security, including its *Report on Money Laundering Typologies* and its *Annual Money Laundering Reports*. Both are available through the Washington, D.C., office of the Organization for Economic Cooperation and Development at 800/456-6323.

The U.S. Treasury Department's Web site (http://www.ustreas.gov) contains a key word search function that allows users to search specific topics, such as "money laundering" or "terrorism." It provides links to other Treasury agencies, including U.S. Customs, Secret Service, FinCEN, and the Office of Comptroller of Currency (OCC).

The OCC link provides information on banking issues, including the names of bankers who have been "prohibited from participating in the business of banking without prior regulatory approval." OCC issuances are available through the OCC's fax-on-demand service (202/479-0141), which includes documents on the Bank Secrecy Act and Currency Transaction Reports.

Also of importance is the IRS's Currency Transaction Report Bulletin Board, which can be accessed by telephoning 313/234-1453.

The FinCEN Web site can be accessed directly at http://www.ustreas.gov/treasury/bureaus/fincen and is particularly useful for money laundering information.

The Office of Foreign Assets Control's (OFAC) "Specially Designated" categories are published in the Federal Register and are available through Lexis/Nexis or directly from the Federal Bulletin Board at 202/512-1387. (enter /GO FAC) or at its Web site (http://fedbbs.access.gpo.gov).

OFAC has a fax-on-demand service (202/622-0077) and a Web site (http://www.ustreas.gov/treasury/services/fac/fac.html) that provide the "Specially Designated" categories and are excellent sources of information on industry regulations and countries such as Cuba, Iran, and North Korea.

The U.S. Department of State's 1997 International Narcotics Control Strategy Report contains a 131-page chapter on money laundering. It is published by the department's Bureau for International Narcotics and Law Enforcement Affairs and is available at the State Department's Web site at http://www.state.gov.

For a review of British money laundering regulations, see *Confiscation and Money Laundering: Law and Practice*, available at the Stationery Office Publications Centre in London.

ultimate objective is to integrate the original dirty money into the stream of commerce so that it can be used as if it were legitimate.

THE CORPORATION SHOULD BE SUSPICIOUS IF THE JURISDICTION OF THE BUYER, ORIGIN OF THE MONEY, AND DESTINATION OF THE SHIPMENT ARE NOT THE SAME.

Smuggling. One method of money laundering occurs when a criminal smuggles ill-gotten cash into a country with lax (or nonexistent) money laundering laws. It is deposited in an offshore bank account and eventually wired back to the United States at a later date. Smuggled cash has been found in bowling balls, coffins, scuba gear oxygen tanks of supposed vacationers, and even in the lining of a traveler's leg cast.

Cash deposits. Money laundering occurs through bank deposits of cash-intensive businesses such as casinos, restaurants, and retail shops. For example, a drug dealer wants to launder proceeds from his sale. He makes a deal with a restaurant owner to pay the owner a commission on the money to be laundered. The owner commingles the dirty money with the business's actual revenues, depositing them together into a single bank account.

Launderers frequently divide the total amount of cash to be laundered into smaller amounts, each under $10,000, to avoid bank report requirements. They make separate deposits into numerous unrelated banks, a procedure dubbed "smurfing." (Smurfing has been found with amounts under $3,000.) Balances from these accounts can be wired into one central offshore account and filtered back to the United States at a later date.

Wire transfers. Wire transfers are faceless, nearly instantaneous, and so abundant that reliably accurate monitoring for suspicious activity is difficult if not impossible. Warning signs can include monies wired into one bank account from various offshore jurisdictions, particularly if monies are wired out of that account in a reasonably short period of time, or large sums of money wired to recently opened bank accounts of individuals and recently established businesses.

Laundering money through wire transfers can involve huge amounts of money and occur over long periods of time. In 1995, for example, a joint task force of federal, state, and city law enforcement (called El Dorado) determined that $1.3 billion had been wired from currency remitters in New York to Colombia throughout the year. This sum of money was a clear warning sign because the approximately 25,500 Colombian households located in New York would have had to wire $50,000 each to Colombia, an extremely unlikely scenario given that the average median household income of this community was $27,000.

Using a provision of the BSA, the Treasury Department issued a Geographic Targeting Order (GTO)—a mechanism used to require increased reporting and record-keeping procedures in a particular geographic area for a limited period of time. In this case, the GTO was issued for money wiring companies in New York that wired funds to Colombia, requiring them to report all transactions over $750.

After the GTO was issued in 1996, wiring from New York to Colombia dropped off drastically. Money launderers instead began smuggling ill-gotten cash to Colombia via plane and boat, where millions of dollars were seized by law enforcement. In the first three months of the GTO, federal authorities saw cash seizures at east coast airports and seaports increase from the $7 million that had been intercepted during the same period the previous year to $29 million, according to newspaper accounts.

Offshore companies. To attract business, many offshore jurisdictions have favorable tax requirements—or none at all. They also have strict privacy laws that do not require the identity of the corporation's officers or principals to be a matter of public record and make it a serious crime for anyone to violate a client's financial confidentiality. While there are legitimate reasons for persons within the United States to establish offshore entities, it is clearly an enterprise ripe for exploitation by money launderers.

Money launderers interested in offshore options need not travel to these locations. They can hire a local service provider to handle the logistics. Some providers even maintain ready-to-purchase shell companies—these "businesses" were incorporated and named several years earlier and are waiting to be purchased, thereby allowing the purchaser to give later investigators the impression of a company with a more substantial business history.

Money launderers frequently wire funds to and from these offshore banks or shell companies. A complex offshore scheme would work as follows: ABC Company, located in an American city, establishes XYZ Corporation in an offshore jurisdiction. ABC then claims to sell its inventory to XYZ, but for a poor profit margin, allowing it to escape paying its full tax burden. XYZ then sells its new inventory on the open market for a substantial profit, which is not taxable in the offshore jurisdiction. The money can then be smuggled into the United States, where it is laundered through a cash-intensive business, or it can be wired to shell companies in other jurisdictions before being wired to the United States. Alternatively, XYZ may agree to put up the money for ABC to use as collateral for a bank loan, thereby allowing ABC Company to benefit while avoiding taxes on its profits.

In another scheme, money earned through drug deals or other illegal activities can be smuggled to an offshore jurisdiction or deposited in an American bank as proceeds from a cash-intensive business. The money is then wired to an offshore account, where it is transferred through a variety of shell companies in various offshore jurisdictions before being wired back to a different American account.

Purchasing goods. As public and private efforts to curtail money laundering at financial institutions have increased, launderers have turned to the nonfinancial sector. According to the FATF report mentioned earlier, "nonbank financial institutions and nonfinancial businesses are becoming more attractive avenues for introducing illicit gains into regular financial channels as the anti-money-laundering regulations in the banking sector become increasingly effective."

Industries such as metals, chemicals, jewelry, artwork, liquor, insurance, consumer electronics and appliances, heavy equipment, and real estate have been targeted as a means for money launderers to exchange dirty money for something of value that could then be sold to an unwitting buyer.

Corporations should be suspicious of

unusual purchase orders from unknown companies located in countries that are recognized operating bases of money launderers or drug dealers. Companies should be on the lookout for red flags such as when orders are placed to more than one sales branch of the same manufacturer, a purchaser seems overly concerned about delivery time, payments are offered in cash or cash equivalents, or an order appears inconsistent with the company's regular business or annual revenue. The corporation should be especially suspicious if the jurisdiction of the buyer, origin of the money, and destination of the shipment are not the same.

SECURITY'S ROLE. Of all company personnel, security directors are the most attuned to suspicious activity and criminal behavior. They are able to recognize suspicious patterns and understand the investigative techniques needed to make necessary assessments. Security professionals, therefore, can play a significant role in protecting their company from being used by money launderers.

The first step in protecting a company is awareness of the problem. The security manager should keep abreast of new laundering trends, targeted industries, and government regulations. While decision makers in the heavily regulated financial sector are cognizant of their legal requirements (banks should have a designated money laundering compliance officer if not a compliance unit), security directors in the nonfinancial sector can be on the forefront of bringing this potential problem to the company's attention.

The security manager should participate in a company's anti-money-laundering activities. For example, the security manager can contribute to a company's training sessions on money laundering trends and investigative techniques. (Training programs are a significant component of a financial institution's money laundering compliance plan.) The security professional can also contribute to formulating a KYC policy.

The security manager should communicate with the company's general counsel. The corporate legal department will be responsible for handling money laundering issues and may be unaware of the security director's potential contribution to dealing with the problem.

The security manager should be familiar with government agencies, such as the Office of the Comptroller of the Currency (OCC), which supervises and regulates national banks, and the Office of Foreign Assets Control (OFAC), a U.S. Treasury Department unit that administers and enforces economic and trade sanctions against certain foreign countries, terrorism sponsoring organizations, and international narcotics traffickers. (The names of these countries and organizations can be found in two OFAC publications: the *Specially Designated Nationals* and the *Specially Designated Narcotics Traffickers* lists.)

While fighting money launderers can be a difficult task for any business, the corporate security manager is well placed to make a significant contribution by knowing the regulations, understanding money laundering techniques, and utilizing his or her personal skills and resources. ■

Richard Horowitz is an attorney and private investigator concentrating in security, corporate, and international issues. He is a member of ASIS.