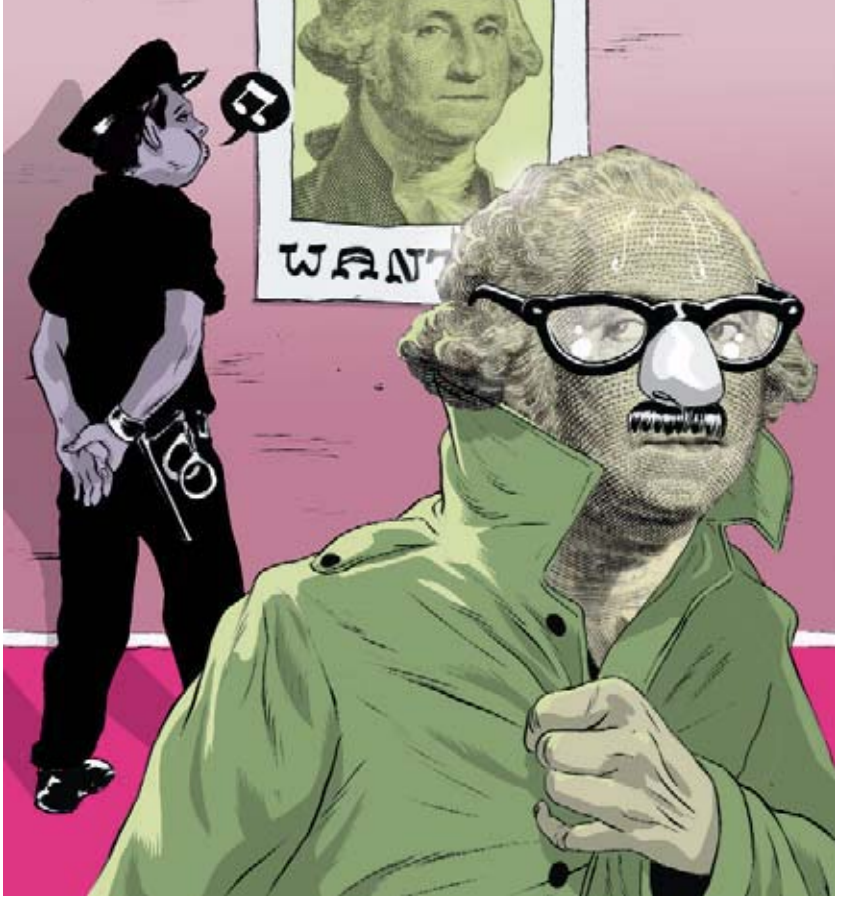
AFTER SEPTEMBER 11, THE FIGHT AGAINST MONEY LAUNDER

dirty money

BY MIRIAM WASSERMAN
ILLUSTRATIONS BY TOMER HANUKA

The first strike against terrorism after the September 11 attacks on the World Trade Center and the Pentagon was a financial one. Not two weeks had passed since the attacks when President Bush signed an executive order freezing the U.S. assets of 27 entities that included terrorist organizations, individual terrorist leaders, a corporation alleged to be a front for terrorism, and several nonprofit organizations. In the days and weeks that followed, policies to impede the covert flow of illicit funds through the global financial system were among the measures at the heart of Congressional debates on how to fight terrorism.

ING HAS ACQUIRED NEW URGENCY



This response should come as no surprise. Measures against money laundering have increasingly become an important front in the fight against crime. Such measures can facilitate detection of financial trails that provide important sources of evidence, potentially linking the members of a criminal organization and leading to convictions of the ring leaders—who are hard to connect to the day-to-day criminal operations. Moreover, finding and seizing money or assets that result from criminal activity can also serve to take the motive out of crime. And, in the case of terrorist financing, it can make it more difficult to commit future acts.

Even before September 11, banks and other financial and nonfinancial institutions in the United States had been required to keep increasingly detailed records of financial transactions and report suspicious dealings. International organizations have worked on designing common standards to fight money laundering and have begun to pressure countries with lax regulations to adopt stricter laws.

Anti-money laundering policies promise to become even more stringent in the aftermath of September 11. The U.S. Congress passed the USA PATRIOT Act, which expanded anti-money laundering provisions. It will affect a broad range of companies, such as securities brokers and dealers, commodity firms, and investment companies. It also imposes more exacting requirements for U.S. financial institutions dealing with foreign customers and institutions, and provides for greater scrutiny to open new accounts at U.S. financial institutions. Many foreign countries are following suit.

But, fighting money laundering is no easy task. With increasing globalization and advances in banking technologies, moving money around the world has become easier and, with the growth in international capital flows, it has also become easier to mask illegitimate monies in the stream of legitimate transfers. Even as nations such as Switzerland and the Cayman Islands have begun to restrict their coveted bank secrecy regimes, nations with underregulated financial systems, such as the Pacific island nation of Nauru, have emerged as centers of importance in the realm of global finance.

Similarly, as new domestic laws have made money laundering more difficult in particular areas of the financial system, criminals have sought new ways to disguise their loot. And, when it comes to terrorism finance, authorities have to think very differently about the issue. Instead of looking for dirty money in the process of being cleansed, they now also have to detect funds that may have legitimate origins but are destined for criminal ends.

MONEY LAUNDERING 101

Criminals have always tried to hide their money. The greater the amount illegally earned, the more difficult it becomes to camouflage its origins and enjoy the proceeds of crime. Sudden, inexplicable wealth can draw the attention of authorities. And, ever since Al Capone was put behind bars for tax evasion, criminals have known that handling and using the spoils of their endeavors can be one of their weakest links.

The practice of disguising wealth, whether legitimate or illegitimate, from government attention has a long history. More than 3,000 years ago, merchants in China protected their wealth from government confiscation using some of the same schemes in use today: converting money to movable assets; moving cash outside a jurisdiction to invest in a business; and trading at inflated prices to expatriate funds, according to a study cited by money laundering expert Nigel Morris-Cotterrill.

Today, nobody knows for sure how much money is laundered globally. It is difficult to know if money is being counted more than once as it cycles through the system and harder still to know how much goes undetected. Nonetheless, experts believe the amounts are large. The most cited figure is between 2 and 5 percent of global GDP—or between $600 billion to $1.5 trillion per year. Still, this is an admittedly rough estimate based on extrapolations of the global sales of illegal drugs on the lower bound, and estimates of the size of underground economies on the upper bound.

To disguise the unlawful nature of funds, criminals must go through a process that varies from crime to crime but that gen-

MANY FIRMS ARE NOW REQUIRED TO REPORT ON SUSPICIOUS ACTIVITIES BY THEIR CLIENTS

erally involves three separate stages. First, cash must be converted into a more portable and less suspicious form—sometimes achieved by using cashier's checks or money orders—and then it is entered into the financial system. Once there, it goes through a series of transactions that resemble legitimate activity and often involve crossing several national borders, making it more difficult for law enforcement agencies to follow the trail. Finally, the funds must be integrated into the legitimate financial system.

Of course, not every criminal act calls for the profits to be laundered. Petty criminals can get away with working in cash. But bigger criminals have to resort to increasingly elaborate methods to create the illusion of legitimate wealth.

Take, for example, the drug trade. Illegal drug trafficking is believed to be the largest source for laundering in the United States and accounts for 60 to 80 percent of all federal money laundering prosecutions, according to James Richards, author of *Transnational Criminal Organizations, Cybercrime, and Money Laundering*. Just the bulkiness of drug money creates logistical problems. Justice Department officials have estimated that the weight of cash generated by drug sales is about ten times that of the drug itself for heroin and six times for cocaine. While traffickers only need to smuggle and distribute about 22 pounds of heroin to net $1 million, they then have to contend with 220 pounds of street cash.

Smuggler caught with $77,000 under his shirt.

JAMES R. TOURTELLOTTE, U.S. CUSTOMS SERVICE

Not surprisingly, the assets of drug traffickers and other criminals who produce vast volumes of cash are believed to be most vulnerable to detection at the stage of placing cash into the financial system. Thus, they often try to avoid triggering the mandatory reporting requirements of large cash transactions by U.S. banks, or steer clear of U.S. financial institutions altogether. Bulk cash smuggling across international borders is perhaps the most widespread way of doing this. Smuggling is done in a variety of ways, from employing an army of couriers who physically transport loads of concealed cash to using trucks and containers.

Once the dollars leave the United States, they can be placed in banks in countries that have weaker controls. Or, cash can simply be brought back into the United States, points out Richards. In this scheme, cash smuggled out of the country is brought back in, this time declared at the border supported by false invoices and receipts. As the funds are recognized by U.S. Customs, they can be deposited at any U.S. bank

THE BLACK MARKET PESO EXCHANGE

Perhaps the largest money laundering system in the United States is the Colombian Black Market Peso Exchange, estimated to launder at least $5 billion a year in drug proceeds. The network has existed for decades as a way to avoid Colombian currency controls and tax laws. Drug traffickers turned to it in order to convert the dollars earned from drug sales in the United States into pesos back home. They sell their dollar proceeds for pesos to brokers who take on the task and the risk of cleaning the money.

The brokers take the dollars at exchange rates usually between 20 and 40 percent below the official Colombian exchange rate. They place the cash in U.S. banks by smurfing or other schemes (see page 18). Then, they sell the dollars in Colombia to importers or businessmen and use the pesos to pay the traffickers in their home turf. The dollars deposited in U.S. banks are wired to personal accounts or used to pay legitimate companies for goods, as Colombian importers often buy American appliances, electronics, car parts, and cigarettes to be smuggled into and sold in Colombia.

In an attempt to disrupt this arrangement, Colombian and U.S. authorities have begun to work with the firms that take the end payments. In summer of 2000, at the request of the U.S. government, Panamanian authorities seized a Bell model 407 helicopter purchased by a Colombian individual from Bell Helicopter Textron, of Fort Worth, Texas. The government also froze payments in the company's bank account, alleging the money was linked to laundering of drug proceeds. The evidence: Bell had received as payment 31 separate wire transfers from individuals and companies with no known relationship to the purchaser of the $1.5 million helicopter. For its part, Bell contended that it did not know that drugs were the source of the funds and that, in its view, it had complied with U.S. laws.

The U.S. government has campaigned to educate U.S. manufacturers and distributors about the forfeiture and indictment they can face if they are caught knowingly participating in the black market scheme. The Colombian government has also been pressuring U.S. companies to look more closely at customers. In 2000, Colombian states went so far as to sue Philip Morris, alleging that its products are frequently smuggled into Columbia as part of the black market exchange, costing the government dearly in lost tax revenues—Colombian police estimate that only 4 percent of Marlboros consumed in the country got there legally, according to *Newsweek*. But companies seeking to comply may face additional costs. General Electric told *Frontline* that, as a result of stricter controls, including not allowing distributors to export out of the country, sales to South Florida decreased by about 25 percent between 1995 and 1999.

without raising red flags. There is some evidence this technique is widespread: Brownsville, Texas, and Nogales, Arizona, had the most funds declared upon entry into the United States from the Mexican border—$8 billion and $5 billion, respectively, between 1988 and 1990—amounts much higher than would be justified by their population or flow of commerce, according to the Financial Crimes Enforcement Network of the U.S. Treasury Department (FinCEN), as cited by Richards.

Launderers have also sought ways to use the U.S. financial system without raising suspicion. Some criminals break down the cash earned into many smaller wads for deposit. This technique came to be called "smurfing" by law enforcement officials in Florida after the little blue cartoon characters. In this method, many people—the smurfs—make large numbers of deposits, always below $10,000, at several different institutions on a daily basis, thus avoiding triggering U.S. bank reporting regulations. (See box on the Colombian Black Market Peso Exchange on page 17.)

Front companies are another common way of placing cash in the system. By running cash-intensive businesses, such as restaurants or liquor stores, launderers can blend legal and illegal profits and make large cash deposits into banks without eliciting questions. In addition, criminals may look beyond banks to businesses such as foreign exchange bureaus, money remittance businesses, and check cashers to convert cash into easier-to-handle instruments or to send the funds abroad.

And, there is also the option of using underground banking structures such as Hawala. Hawala is an old system that originated in South Asia but now operates in many countries. Such informal financial networks are very attractive to those seeking to transfer money without government notice because the transactions leave no paper trail. A person who wants to send money abroad takes the cash to an underground banker who gives him a marker or some form of receipt. The broker in turn, informs his contacts in the transfer's destination so that the designated receiver can claim the money at the other end, minus a commission. The money does not physically need to be transported abroad, as two-way flows support the exchange: Cash for the payment is provided by customers wanting to send money in the opposite direction.

A WORLD OF OPPORTUNITIES

Once the money is placed in the financial system somewhere in the world, technology and globalization facilitate the process of disguising the origin of the funds and reintegrating them into the realm of legitimate finance. Wire transfers, for instance, offer launderers the possibility of quickly moving money through different accounts and different countries until it becomes impossible to trace the origin of the funds. One of the most recent trends, according to the U.S. Treasury, involves funds wired to or through a U.S. financial institution—primarily from Switzerland, Italy, Germany, and England—and then withdrawn in any one of about 57 nations through an automated teller machine (ATM). The largest number of this type of ATM withdrawals is made in Colombia.

Another way in which funds deposited abroad can be repatriated and given a semblance of respectability is through loans. Illicit funds deposited in foreign banks can be used as collateral for loans drawn for legitimate investments elsewhere.

Furthermore, criminals have increasingly resorted to products and services in so-called offshore banking havens such as Nauru. These jurisdictions tend to offer a certain level of banking or commercial secrecy, low or no tax rates, and relatively simple requirements for licensing and regulating banks and other businesses. Money launderers often take advantage of laws that favor easy incorporation and the use of nominee owners or bearer shares—which allow anonymous ownership of companies. Such laws allow them to create "shell" companies that do not conduct any commercial or manufacturing business and whose sole purpose is to serve as conduits for fund flows.

Whatever the "cleansing" method, the transactions involved are usually extremely complicated—and deliberately so. In the investigation of alleged money laundering by Raul Salinas (the brother of the former Mexican president), for instance, the U.S. Government Accounting Office (GAO) found that Mr. Salinas

TECHNOLOGY AND GLOBALIZATION HAVE PROVEN HELPFUL TOOLS FOR HIDING ILLEGAL WEALTH

was able to transfer between $90 million and $100 million between 1992 and 1994 from Mexico to London and Switzerland through a private banking account with Citibank in New York. Key in enabling him to do this was a private investment company in the Cayman Islands named Trocca, which was formed by Cititrust (Cayman), then an affiliate of Citicorp—now known as Citigroup—to hold Mr. Salinas's assets. The laws in the Cayman Islands protected the confidentiality of the documentation linking Mr. Salinas to Trocca. To further insulate Mr. Salinas's connection to Trocca, "Cititrust (Cayman) used three additional shell companies to function as Trocca's board of directors—Madeleine Investments SA, Donat Investments SA, and Hitchcock Investments SA," states the GAO report. In addition, many of the fund transfers from Mexico to New York were made by Mr. Salinas's wife using her maiden name. The whole affair was only discovered after Mr. Salinas was arrested and charged with murder in 1995. (In 1999, Raul Salinas was sentenced to 50 years in prison in Mexico on charges of planning the 1994 murder of Jose Francisco Ruiz Massieu, his former brother-in-law and a leader of the Institutional Revolutionary Party.)

THE CAT-AND-MOUSE GAME

In spite of money laundering's long history and broad impact, laws against the practice are relatively recent in the United States—and even more so in other countries. Money laundering was not considered a federal crime in the United States until the mid 1980s. The term itself first appeared in print in the early 1970s in the context of the Watergate scandal, when it was used to describe a process to circumvent a law prohibiting anonymous campaign contributions, according to Jeffrey Robinson, author of *The Laundrymen: Inside Money Laundering, the World's Third-Largest Business*. Members of Nixon's Committee to Reelect the President used a contact who received donations in Mexico and then forwarded them to Bernard L. Barker, a real estate salesman in Miami, to protect the identity of the private citizens that made the donations. When Barker was arrested for breaking into the Democratic National Committee headquarters in the Watergate building, the money trail helped link the Watergate break-in back to Nixon.

The growth of the illegal drug trade—with the vast illicit fortunes it generated—was the main factor motivating the evolution of anti-money laundering legislation in the United States and Europe. Reports of people depositing bags of currency of doubtful origin into banks led Congress to pass the Bank Secrecy Act (BSA) in 1970—the backbone of domestic money laundering legislation. Though it did not make laundering a criminal activity, the Act required financial institutions to create and preserve a paper trail for various financial transactions in order to facilitate criminal, tax, or regulatory investigations. As a result, financial institutions have to file reports for most cash transactions over $10,000 and keep such records for five years; and individuals have to report whenever they physically carry more than $10,000 in monetary instruments (coins, currency, travelers' checks, bearer bonds, securities, and negotiable instruments) into or out of the United States.

But criminals would not be deterred and money laundering methods evolved to circumvent these new restrictions. As launderers developed new methods, new laws and more stringent punishments were crafted to cover the regulatory gaps. As it became more difficult to make large cash deposits in banks, for instance, criminals found other businesses that served their needs such as check cashers or money remitters. In response, the currency reporting requirement of the Act was expanded to cover check cashers, currency exchange businesses, casinos, the U.S. Postal Service, and businesses that issue, sell, or redeem traveler's checks, among others. Nonetheless, the reporting requirement was "widely disregarded until 1985," writes Robinson. That year, Bank of Boston was fined $500,000 for not reporting 1,163 transactions valued at $1.2 billion.

In order to further strengthen the fight against dirty money, Congress made money laundering a crime in its own right with the passage of the 1986 Money Laundering Control Act (MLCA). The legislation made money laundering punishable by up to 20 years in prison, provided for both civil and criminal forfeitures of funds, and made it illegal to break down financial transactions to avoid triggering currency transaction reports.

The MLCA defined money laundering fairly broadly. Financial transactions that ordinarily would not be considered illegal became criminal if they knowingly involved the proceeds of a "specified unlawful activity." These activities comprise a long, and expanding, list of over 200 criminal offenses including such diverse items as health care fraud, counterfeiting, drug trafficking, espionage, extortion, murder, and—since 1996—terrorism. (Interestingly, tax evasion is not currently part of the list. So, for instance, a doctor not reporting all his income and sending what he doesn't report to an offshore bank would not be considered to be laundering money unless the money was illegally earned. The Internal Revenue Service recently estimated that as many as one to two million Americans may be evading taxes by secretly depositing money in tax havens like the Cayman Islands and withdrawing it using American Express, MasterCard, and Visa cards.)

Specifically, the MLCA made it a crime to knowingly conduct transactions above $10,000 with property derived from a specified crime. For lower amounts, transactions are illegal if they are intended to conceal the origin of the funds, avoid reporting requirements, or conceal *illegal* proceeds from tax au-

thorities. For any amount, it is also considered money laundering when a monetary transaction into or out of the United States is being carried out with the intent to facilitate a future crime from the specified list. So, in the case of terrorism, even if the funds originated in a "legitimate" donation, their transportation, transfer, or transmission is considered money laundering if they are used to support a criminal cause.

In addition to the passage of the MLCA, the reporting requirements imposed by the Banking Secrecy Act have been expanded. The Annunzio-Wylie Anti-Money Laundering Act of 1992 made it mandatory for financial institutions to report *any* suspicious transactions relevant to possible violations of the law by their clients. As of January 2002, this also included money service businesses, such as issuers of money orders and traveler checks. The law explicitly prohibited banks from informing their customers when they have filed a suspicious activity report. And, it protected banks from civil liability for doing so, by furnishing them with certain "safe harbor" provisions.

Though domestic laws have become increasingly strict, their effectiveness has been limited to the extent that other countries' laws are lax. Just as money laundering techniques spread from banks to other firms in the attempt to circumvent regulation, money laundering activity spread to other countries where the laws were weaker. In fact, some nations developed a large industry based on laws that benefited financial secrecy and discouraged international law enforcement cooperation. The tiny Pacific island of Nauru, which sits halfway between Hawaii and Australia with a population of merely 12,000, for instance, allowed people to set up banks for as little as $25,000 without even setting foot on the island. The nation has been accused of facilitating the laundering of $70 billion in Russian Mafia money through almost 450 banks based there (all registered to the same government post office box).

At issue are not just small nations looking to make quick wealth. There are also international differences in how countries define money laundering and the crimes they accept as underlying unlawful activities. Countries tended to consider only those crimes that had the most pernicious effects on their own soil. The United States, for example, included foreign drug trafficking as an underlying offense, but foreign corruption was not on the list until the USA PATRIOT Act was passed.

Resolving these differences requires international cooperation. From the IMF to the United Nations, several international organizations have taken initiatives against money laundering. Chief among them, the Financial Action Task Force (FATF), created in 1989 by the G-7 (the group of the world's largest industrialized nations, including the United States), which has worked to establish international standards against money laundering. Most recently, the strategy of the FATF members shifted towards a more active role. The organization has named 19 "noncooperative" jurisdictions hoping that increased international scrutiny would pressure them to make their anti-money laundering laws and enforcement practices stronger. In December of 2001, FATF imposed countermeasures on Nauru, deeming that it had not adequately addressed the legal deficiencies in its offshore banking sector.

COSTS AND CONSEQUENCES

The fight against money laundering has not been uncontroversial. Like all legislation, money laundering laws have to play a delicate balance between the costs to businesses and individual citizens with the benefits of legislation. To some critics, the reporting requirements impose high costs on banks and other financial institutions. Though numbers are unreliable, as procedures vary somewhat by institution, the U.S. Treasury's Financial Crimes Enforcement Network estimated in 1999 that it costs financial institutions $109 million a year to comply with the reporting and record-keeping requirements of the Banking Secrecy Act. But whether these costs are high depends on our estimate of the costs crime and laundering impose on society, and on the law's effectiveness in combating them.

The legal definition of money laundering and the penalties imposed by the law have also raised some questions. For instance, the MLCA can make the defense of some alleged crim-

PREVENTING CRIME WHILE PROTECTING PRIVACY REQUIRES AN INCREASINGLY DELICATE BALANCE

inals, such as drug traffickers, a difficult issue for lawyers. An attorney who receives over $10,000 in fees can be accused of money laundering, given that it would be difficult to prove ignorance of the potentially tainted origin of the funds. Precisely because of their problematic nature, prosecutions of this type are rare and have to be approved by the Justice Department.

In addition, the criminal penalties for money laundering drew fire because they were often higher than for other white-collar crimes such that defendants received higher sentences than if charged only with the underlying criminal offense. In response to the criticisms, the sentencing guidelines for money laundering were revised this past November to make punishments more sensitive to the seriousness of the underlying crimes.

But perhaps the most controversial aspect has been the effect that money laundering laws have on privacy and how they affect business-client relationships. The fact that financial institutions and other businesses are obligated to report suspicious transactions to the government changes the nature of their relationship with their clients. It places some businesses that traditionally served clients in confidence partly on the side of enforcement. Moreover, in some cases, it requires that businesses ask more questions of their clients. In order to be able to report suspicious transactions, financial institutions have to make sure they know their customers well. They are expected to conduct a risk assessment and determine the appropriate level of due diligence. In some instances, this might include verifying a customer's identity, determining their sources of wealth, reviewing their credit and character, and understanding the type of transactions the customer would typically conduct.

For banks, which were subject to these regulations well before September 11, the key issue is to make sure they tell customers about what they do and why they do it, says John Byrne, Senior Federal Counsel and Compliance Manager at the American Bankers Association. "You want to be able to explain to your consumer: We don't share or sell your information or, we do, if you allow it," says Byrne. Banks also have to make clear that, if they ask clients for information, they do so to "protect the institution, to protect the country, and to protect the client."

Some European countries and Canada have imposed suspicious activity reporting that goes well beyond the financial sector—requiring attorneys to report on suspicious transactions by clients. This February, the American Bar Association issued a statement urging the government to protect the principle of lawyer-client confidentiality in its fight against money laundering. Other countries have adopted laws or policies that make lawyers "the eyes and ears of the government," Washington, D.C., lawyer Stephen Saltzburg told the media. "This is the single most alarming threat to the attorney-client privilege that anyone has seen in a long time," Saltzburg said.

In the future, balancing our concerns for privacy with the need to prevent crime and terrorism will continue to be one of the most difficult issues in dealing with money laundering. As the evolution of money laundering legislation shows, increased efforts and widened scope are certain to make money laundering more difficult. But, they are not likely to end it. So long as crime exists, the fight against money laundering is likely to continue to be a cat-and-mouse game with new methods and loopholes being discovered as soon as prior regulatory gaps are closed. In this context, money laundering laws and awareness of the issue help prevent innocent citizens and organizations from being corrupted by easy money or from becoming unwitting accomplices to crime. The alternative is to turn a blind eye and let corruption flourish. ❊

CORRUPTING POWER

Law enforcement and financial authorities have focused on money laundering, in part, as a way of combating crimes ranging from drug and arms trafficking to terrorism, fraud, and embezzlement. But, beyond serving as an enforcement tool to combat other crimes, large-scale money laundering poses problems in and of itself. As criminals try to find ways to legitimize large amounts of money, this creates the potential for corrupting government officials and financial institutions. And, even if money laundering does not corrupt the whole institution, banks can see their reputations tarnished and the public's trust in them eroded if they are embroiled in a money laundering scandal.

There can also be macroeconomic consequences. "Money laundering allocates dirty money around the world not so much on the basis of expected rates of return but on the basis of ease of avoiding national controls," says International Monetary Fund economist Vito Tanzi. Thus, money is not used where it is most productive. Moreover, though there are no clear examples of this so far, large and sudden movements of dirty money—say, responding to changes in legislation or law enforcement—could lead to instability in particular countries or banking systems.

In addition, money laundering can end up undermining the legitimate private sector; front companies used to hide ill-gotten gains may offer their services at discounted prices, crowding out legitimate businesses. Hotels and restaurants built to serve as cover for illicit cash may be created in tourist markets that are already saturated. In Colombia, large-scale smuggling of electronic appliances, cigarettes, and other goods is one way in which drug proceeds are introduced into the country. These items are sold at very discounted prices, weakening the domestic manufacturing industry.