

2. MONEY LAUNDERING

TRADITIONAL MONEY LAUNDERING PROCESSES

Money laundering is an illegal activity through which criminal proceeds take on the outward appearance of legitimacy. It is an integral support function common to virtually all profit-producing criminal activities. The U.S. Criminal Code contains more than 100 predicate offenses to the crime of money laundering. These offenses, referred to as “specified unlawful activities,” range from narcotics trafficking and financial fraud, to kidnapping and espionage.

In most financial transactions, there is a financial trail to link the funds to the person(s) involved. Criminals avoid using traditional payment systems, such as checks, credit cards, etc., because of this paper trail. They prefer to use cash because it is anonymous. Physical cash, however, has disadvantages. It is bulky and difficult to move. For example, 44 pounds of cocaine worth \$1 million equals 256 pounds of street cash worth \$1 million. The street cash is more than six times the weight of the drugs. The existing payment systems and cash are both problems for criminals. Even more so for large transnational organized crime groups. Regulations and banking controls have increased costs and risks.

The physical movement of large quantities of cash is the money launderer’s biggest problem. To better understand the potential for abuse of Cyberpayment systems to launder money, a brief explanation of how criminals “legitimize” cash through the traditional money laundering process is provided.

Placement, layering and integration are terms used by law enforcement to describe the three stages through which criminal proceeds are laundered.

Placement. Placement is the first stage in the money laundering process. It is during the placement stage that physical currency enters the financial system and illegal proceeds are most vulnerable to detection. When illicit monies are deposited at a financial institution, placement has occurred. The purchase of money orders using cash from a criminal enterprise is another example of placement. The Bank Secrecy Act (BSA) (see Table 2.1) and related regulations mandate the reporting of certain types of financial transactions which involve cash and/or certain monetary instruments. To conceal their activities money launderers must either circumvent the legitimate financial system entirely, or violate reporting/record-keeping rules established under the BSA. Accordingly, law enforcement officials, working in cooperation with the financial industry, are in a unique position to combat money laundering during this stage.

Layering. Layering describes an activity intended to obscure the trail which is left by “dirty” money. During the layering stage, a launderer may conduct a series of financial transactions in order to build layers between the funds and their illicit source. For example, a series of bank-to-bank funds transfers would constitute layering. Activities of this nature, particularly when they involve funds transfers between tax haven and bank secrecy jurisdictions, can make it very difficult for investigators to follow the trail of money.

Integration. During the final stage in the laundering process, illicit funds are integrated with monies from legitimate commercial activities as they enter the mainstream economy. The illicit funds thus take on the appearance of legitimacy. The integration of illicit monies into a legitimate economy is very difficult to detect unless an audit trail had been established during the placement or layering stages.

TABLE 2.1
The Bank Secrecy Act

The Bank Secrecy Act (BSA), authorizes the Secretary of the Treasury to issue regulations requiring financial institutions to keep certain records and file certain reports, and to implement anti-money laundering programs and compliance procedures. For the purposes of the BSA, “financial institution” is defined broadly to include, inter alia, a bank, a broker or dealer in securities, a currency dealer or exchanger, or a casino.

The BSA was enacted in 1970 in response to concern over the use of financial institutions by criminals to disguise the proceeds of their illicit activity. The purpose of the BSA and its implementing regulations is to provide law enforcement authorities with the tools necessary to combat these problems by “requiring certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.” Reports required under the BSA include: suspicious activity reports, currency transaction reports, reports of cross-border movements of currency and monetary instruments, and reports on foreign bank accounts. Two of these BSA reports are described below:

Currency Transaction Report (CTR): Covered financial institutions must file a CTR for each transaction in which they are involved that exceeds \$10,000. Under this requirement, multiple currency transactions are treated as a single transaction if they total more than \$10,000 during any one business day. The \$10,000 reporting threshold may, in certain circumstances, be modified by the Secretary, (see discussion of Geographic Targeting Orders in Chapter 6)

Report of International Transportation of Currency and Monetary Instruments (CMIR): Each person must make a CMIR declaration when he or she physically transports currency or other monetary instruments in an aggregate exceeding \$10,000 at one time, into or out of the United States.

Generally, a person willfully violating the BSA or its implementing regulations is subject to a criminal fine up to \$250,000 or a five-year term of imprisonment, or both. A person who makes such a violation while violating another law of the United States, or engaging in a pattern of illegal activity, is subject to a criminal fine of up to \$500,000 or a ten-year term of imprisonment, or both.

MONEY LAUNDERING SCHEMES

Money laundering schemes may vary greatly in character and complexity. They may involve any number of intermediaries and utilize both traditional and non-traditional payment systems. To a large extent, the scope and nature of a money laundering operation is limited only by the creativity of those involved. International narcotics traffickers may employ a variety of different money laundering techniques and schemes at any one time, each specially created to fulfill specific goals and objectives.

Advanced computing and communications technologies are currently routinely used to enhance the efficiency and the security of narcotics-related money laundering operations.

The examples which follow below are base-line schemes intended to familiarize the reader with a few simple methods for moving illicit funds.

Example #1 (Figure 2.1): Move U.S.-based funds to Mexico for use in local economy.

1. Street level narcotics sales occur in the U.S. (cash is the preferred method of payment for these transactions.)
2. The cash from one or multiple sales locations is collected at a safe or “stash” house for processing.
3. The cash is taken to a remittance business for transmission out of the country. To avoid scrutiny by law enforcement or bank regulatory authorities, the cash may be divided into amounts less than \$10,000 and “smurfed” (the employment of a large number of individuals to make small deposits and withdrawals) or structured (transfer of amounts below federal reporting requirements) at the remittance business.
4. The funds are sent by the U.S.-based remitter to a Mexican-based counterpart. (The remittance company will normally utilize an offsetting book entry transfer or conduct a bank wire transfer in order to move the money out of the United States.)
5. The remittance business in Mexico pays out in Pesos.

Example #2 (Figure 2.2): Move Laundered Funds from U.S. to Mexico.

1. Money from U.S. drug sales is converted into money orders.
2. Money orders are shipped to Colombia via express mail.
3. U.S. funds money orders are sold to a currency broker in exchange for Pesos.

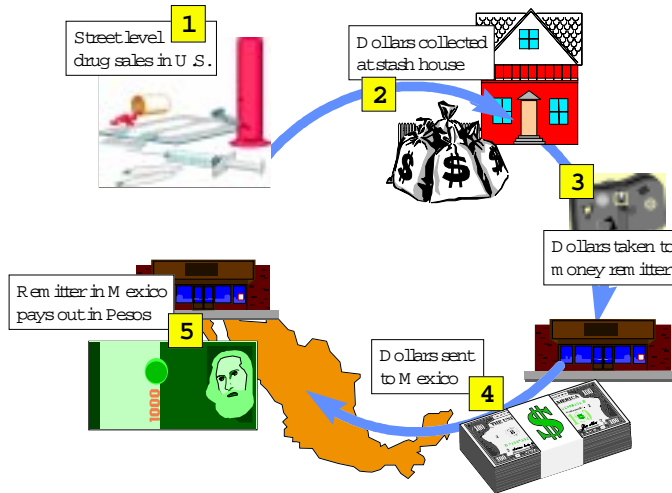


Figure 2.1. Movement of Funds from the U.S to Mexico

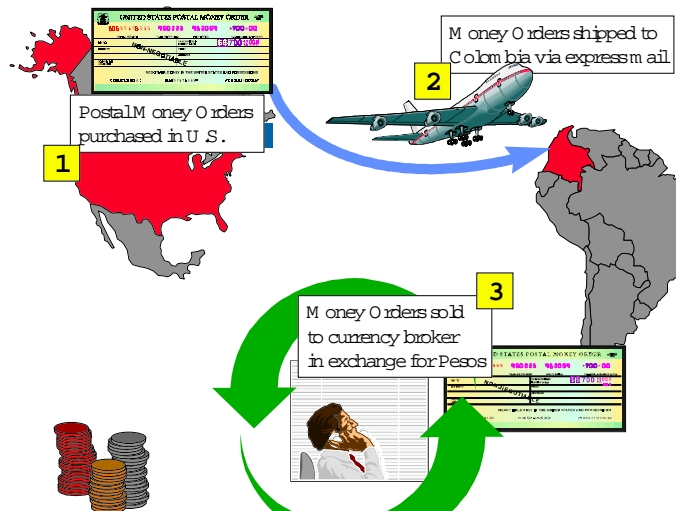


Figure 2.2. Move Laundered Funds from the U.S. to Mexico

GEOGRAPHIC TARGETING ORDERS AND ANTI-MONEY LAUNDERING POLICIES

The speed and “paperless” nature of Cyberpayment transactions pose potential challenges for traditional methods of policing illegal cash transactions. These methods of preventing, detecting, and combating money laundering are characterized by techniques that require large numbers of personnel. Extensive coordination of law enforcement activities among federal, state, and local police agencies is also critical to the effective implementation of anti-money-laundering initiatives.

A Geographic Targeting Order (GTO) is one technique used by law enforcement authorities to investigate money-laundering activities relating to drug trafficking. A GTO gives the Treasury Department the authority to require a financial institution or a group of financial institutions in a geographic area to file additional reports or maintain additional records above and beyond the ordinary requirements imposed by BSA regulations.

A GTO initiated in New York in 1996 (and extended into 1997) required at one point, 23 money transmitters and their approximately 3200 agents to report identifying information on all cash remittances of \$750 or more to Colombia. This led to a dramatic reduction in the volume of suspected drug related funds flowing through money transmitters to Colombia, and triggered a number of large seizures of cash at air and sea ports along the eastern seaboard as traffickers shifted to more vulnerable means of moving their money.

A GTO thus has at least two important and complementary functions. First, it serves as an information gathering device that enables law enforcement authorities to gain greater knowledge of patterns of money laundering. The information gathered helps to establish better estimates of the volume of illicit funds laundered, and assists in more effective targeting of illegal activities by law enforcement. Second, a GTO helps to prevent evasion of the BSA regulations by disturbing established patterns of money laundering through the introduction of uncertainty and heightened risk into the cost-benefit and other calculations of drug traffickers and others who would circumvent the standard BSA reporting and record keeping requirements. This preventive function is a significant part of the value of GTOs to law enforcement’s anti-money laundering efforts.

The physical movement of cash remains a critical weak point in drug trafficker attempts to launder illicit funds. Targeting particularly vulnerable industries or industry segments -- such as money transmitters sending funds to Colombia -- increases the transparency of a particular type of financial transaction while also creating a “money disposal” problem for drug traffickers. This implicit rise in the “price” of handling cash derived from illegal activities is a key variable in the “economics” of the drug business. In this sense, price shifts in the cost of money laundering may cause money launderers to seek alternative ways to move their funds into the legitimate financial systems.

GTOs AND NEW PAYMENT SYSTEM TECHNOLOGIES

GTOs have been implemented four times -- in Phoenix in 1989, in Houston in 1991, in New York from August 1996 to October 1997, with respect to cash purchased remittances to Colombia, and in New York and Puerto Rico from September 1997 to the present with respect to cash purchased remittances to the Dominican Republic. The success of the Colombia operation

is attributable in large part to the commitment of considerable resources and personnel to its planning, implementation and follow-up. Even if resource limits *did not* restrict the use of these methods, their long-term utility could be affected by the emergence of Cyberpayment system technologies.

Law enforcement techniques may need to adapt very rapidly to these emerging technical possibilities while at same time seeking to maximize the effectiveness of existing investigative techniques. The development of new law enforcement investigative techniques is a necessary complement to the continuing utility of traditional investigative methods. Consistent with concerns for minimizing the cost of oversight requirements on Cyberpayment system operators, proposed governmental regulations were evaluated by industry participants during the exercise process. In addition, Cyberpayment industry representatives were consulted throughout the exercise design process with a view to assessing the technical feasibility of proposed investigative techniques against the known (though dynamic) characteristics of deploying Cyberpayment systems.