International Narcotics Control Strategy Report -2003

Released by the Bureau for International Narcotics and Law Enforcement Affairs
March 2004

Money Laundering Methods, Trends and Typologies

As in previous years, money launderers and supporters of terrorism have demonstrated great creativity in combining traditional money laundering techniques into complex money laundering schemes designed to thwart the ability of authorities to prevent, detect and prosecute money laundering. Below is a review of U.S. money laundering trends in 2003 and examples of the various money laundering/terrorist financing typologies.

Statistical Overview of U.S. Money Laundering Trends in 2003

The U.S. Suspicious Activity Reporting System plays a critical role in U.S. anti-money laundering efforts. Similar types of reporting throughout the world are key to global efforts to combat money laundering. The aggregate totals for U.S. Suspicious Activity Reports (SARs) help illustrate the nature of illegal proceeds and the relative scale of the problem. Depository institutions (i.e., banks, thrifts, savings and loans, and credit unions) have been required to file SARs since 1996. The USA PATRIOT Act extended the mandatory reporting requirements to brokers and dealers in securities, and the Department of the Treasury, pursuant to its rulemaking authority, extended it to casinos and money services businesses (MSBs), including money exchangers, sellers of traveler's checks and money transmitters.

The requirements went into effect on January 1, 2002 for MSBs, on January 1, 2003 for brokers and dealers in securities, and on March 25, 2003 for casinos. The regulations generally require that covered financial institutions file a SAR when they suspect violations of law or suspicious activities involving amounts greater than between $2,000 and $5,000, depending on the institution's applicable reporting threshold. The following chart provides aggregate totals for SARs filed by depository institutions (i.e., banks, thrifts, savings and loans, and credit unions) from April 1, 1997 through June 2003. Additionally, a small part of the total volume relates to reports filed by affiliates of depository institutions or, in some cases, filed voluntarily by MSBs; by brokers and dealers in securities who were not affiliated with banks; or by gaming businesses that, during the time period, were not yet required under the Bank Secrecy Act (BSA) to file SARs.

From inception of the SAR requirement in April 1996 through June 2003, a total of 1,126,488 SARs were filed, with the volume of filings increasing from 52,069 during 1996 to 273,823 in 2002. During the first six months of 2003, 136,115 SARs were filed.

Financial institutions identifying suspicious transactions under the Bank Secrecy Act of 1970, chapter 53 of title 31, United States Code (BSA) are required to report such transactions by

filing a SAR with the Financial Crimes Enforcement Network (FinCEN), in accordance with applicable regulations. SARs are not proof of illegal activity; rather they note possible wrongdoing that warrants further investigation. An actual determination of criminal activity can only be made following an investigation by law enforcement of the activity addressed in the SAR.

Table 1: Frequency Distribution of SAR Filings by Characterization of Suspicious Activity

April 1, 1997 Through June 30, 2003

Violation Type	1997	1998	1999	2000	2001	2002	2003
BSA/Structuring/Money Laundering	35,625	47,223	60,983	90,606	108,925	154,000	72,462
Bribery/Gratuity	109	92	101	150	201	411	261
Check Fraud	13,245	13,767	16,232	19,637	26,012	32,954	16,803
Check Kiting	4,294	4,032	4,058	6,163	7,350	9,561	5,333
Commercial Loan Fraud	960	905	1,080	1,320	1348	1,879	934
Computer Intrusion[1]	0	0	0	65	419	2,484	3,605
Consumer Loan Fraud	2,048	2,183	2,548	3,432	4,143	4,435	2,271
Counterfeit Check	4,226	5,897	7,392	9,033	10,139	12,575	6,445
Counterfeit Credit/Debit Card	387	182	351	664	1,100	1,246	659
Counterfeit Instrument (Other)	294	263	320	474	769	791	615
Credit Card Fraud	5,075	4,377	4,936	6,275	8,393	12,780	6,037
Debit Card Fraud	612	565	721	1,210	1,437	3,741	4,575
Defalcation/Embezzlement	5,284	5,252	5,178	6,117	6,182	6,151	2,887
False Statement	2,200	1,970	2,376	3,051	3,232	3,685	2,316
Misuse of Position or Self Dealing	1,532	1,640	2,064	2,186	2,325	2,763	1,564

Mortgage Loan Fraud	1,720	2,269	2,934	3,515	4,696	5,387	3,649
Mysterious Disappearance	1,765	1,855	1,854	2,225	2,179	2,330	1,264
Wire Transfer Fraud	509	593	771	972	1,527	4,747	4,317
Other	6,675	8,583	8,739	11,148	18,318	31,109	15,854
Unknown/Blank	2,317	2,691	6,961	6,971	11,908	7,704	2,290
Totals	**88,877**	**104,339**	**129,599**	**175,214**	**220,603**	**300,733**	**154,141**

[1]The violation of Computer Intrusion was added to Form TD F 90-22.47 in June 2000. Statistics date from this period.

General Money Laundering Trends in 2003

Organized crime and narcotics-traffickers have used the following methods for decades to launder their illegal proceeds. These methods continue to be used frequently.

- Financial activity inconsistent with the stated purpose of the business;
- Financial activity not commensurate with stated occupation;
- Use of multiple accounts at a single bank for no apparent legitimate purpose;
- Importation of high dollar currency and traveler's checks not commensurate with stated occupation;
- Significant and even dollar deposits to personal accounts over a short period;
- Structuring of deposits at multiple bank branches to avoid Bank Secrecy Act requirements;
- Refusal by any party conducting transactions to provide identification;
- Apparent use of personal account for business purposes;
- Abrupt change in account activity;
- Use of multiple personal and business accounts to collect and then funnel funds to a small number of foreign beneficiaries;
- Deposits followed within a short period of time by wire transfers of funds;
- Deposits of a combination of monetary instruments atypical of legitimate business activity.
- Movement of funds through countries that are on the FATF list of NCCTs.

As in previous years, money launderers have demonstrated great creativity in combining traditional money laundering techniques into complex money laundering schemes designed to

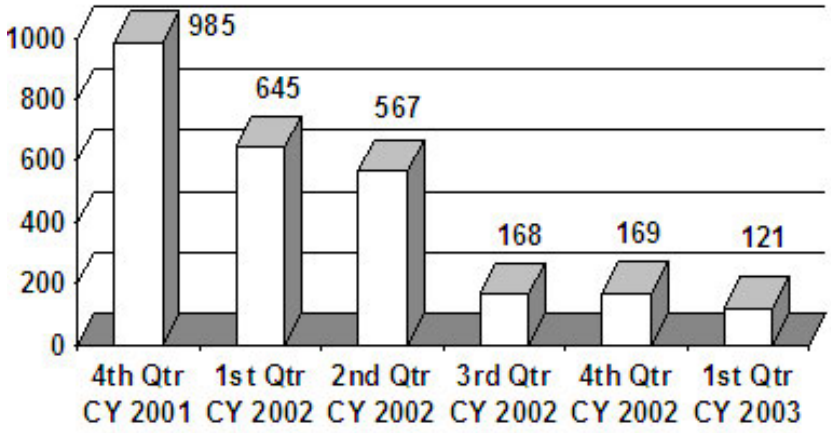
thwart the ability of authorities to prevent, detect and prosecute money laundering. Following is a review of U.S. money laundering trends in 2003 including examples of the various money laundering and terrorist financing typologies.

SARs Relating to Terrorist Financing

FinCEN continues to examine the SAR database to determine the extent to which SARs have been filed by institutions that suspect certain activities may relate to terrorism and terrorist financing. A recent review identified several interesting trends. First, the number of SARs submitted from financial institutions reporting suspected terrorism or terrorist financing has continued to decline steadily since the events of September 11, 2001. Secondly, of all SARs filed referencing terrorism, one-third were filed as a result of names appearing on government lists (Office of Foreign Assets Control or OFAC—or other watch lists) or in response to USA PATRIOT Act Section 314(a) information requests. Finally, the remaining two-thirds of all SARs reviewed appeared to be submitted as a direct result of proactive initiatives by institutions, which are becoming more aware of possible indicators of financial activity and transactions by suspected terrorists and terrorist organizations. In other words, institutions are becoming less dependent on specific lists and are identifying on their own suspicious activity as being potentially terrorist-related. This section offers a synopsis of SAR statistical data for the recent review period and identifies the general types of activities being reported in terrorist-related SARs.

Chart 1: SARs filed relating to terrorism for the 18-month period (by Calendar Year quarters)

October 1, 2001 thru March 31, 2003



As the above chart demonstrates, the number of filings began to steadily decline after the 4th quarter of calendar year 2001, the three-month period directly following the September 11th terrorist attacks.

Following is additional information about the 290 SARs filed between October 1, 2002 and March 31, 2003 (the last six months of the study) that reference terrorism and/or terrorist financing:

- Sixty-nine financial institutions, including five foreign banks licensed to conduct business in the United States, filed SARs (three banks filed 155 of the 290 SARs or 53.4 percent of the SARs filed).

- The suspicious activity reported in the SARs occurred in 35 states and the District of Columbia.
- Alleged suspicious activity amounts ranged up to $193 million.

Eighty-four SARs (29 percent) filed were the result of apparent matches of names on OFAC's list of Specially Designated Nationals and Blocked Persons, from the USA PATRIOT Act's Section 314(a) Information Requests from law enforcement, names gleaned from media reports, or as a result of subpoenas issued by law enforcement.

The activity described in the SARs remained consistent with the activity described in previously issued SAR Review Reports. The activity included wire transfers predominantly to and from Middle Eastern countries; frequent use of domestic and foreign Automated Teller Machines (ATMs); and large currency transactions. The majority of the SARs filed (206 SARs or 71 percent) were a result of depository institutions' discoveries during the due diligence process. This denotes the first time since the events of September 11, 2001, that a marked increase in independent depository institution filings occurred, i.e., without the aid of government published lists. It is also worth noting that, previously, the filings were reversed in that 75 percent to 80 percent were filed based on government watch lists, while 20 percent to 25 percent were filed at the depository institutions' initiative.

The above-mentioned SARs were filed based on one or more of the following criteria, which the financial institution believed might be associated with terrorist activity:

- Even dollar deposits followed by like-amount wire transfers;
- Frequent domestic and international ATM activity;
- No known source of income;
- Use of wire transfers and the Internet to move funds to and from high risk countries and geographic locations;
- Frequent address changes;
- Occupation "student"—primarily flight schools;
- Purchases of military items or technology; and
- Media reports on suspected/arrested terrorists or groups.

Alternative Remittance Systems (ARS)

In 2003, FinCEN completed an analysis of a sampling of SARs referencing ARS or ARS-like operations. Four predominant themes identified from those SARs are:

- Unlicensed and/or unregistered money transmitters;
- Hawala or other types of ARS;
- Black Market Peso Exchange (BMPE); and,
- Evasion of the International Emergency Economic Powers Act (IEEPA).

Illegal Money Transmitter Businesses

Forty-five SARs (or 56.3 percent) filed regarding unregistered and/or unlicensed money transmitter businesses identified a variety of techniques commonly used by ARS operators to facilitate the transfer of funds on behalf of their customers. Many unlicensed/unregistered money transmitters were identified by the filing institution as ARS because of the mechanisms used to conduct transactions that ultimately ended up going through a depository institution account, such as aggregation of monetary instruments or cash from multiple sources. Most ARS operations are considered Money Services Businesses (MSBs) by virtue of the funds/value transfer services they provide to their customers. The type of account activity exhibited by such entities also provides significant insight into the identification of illegal and informal MSBs that may be providing ARS services. The SARs analyzed for this study provided a number of such indicators:

- Account activity inconsistent with the type of account held by a customer and/or volume of activity anticipated by the filing institution (according to the expected levels conveyed to the institution by the account holder);
- Account holder occupation inconsistent with the type and volume of financial activity affecting an account; e.g. unemployed, housewife, etc.;
- Large volume deposits of cash, checks, and other types of monetary instruments immediately followed by wire transactions abroad; sometimes, multiple wire transfers sent from unregistered and/or unlicensed MSBs to benefit a single beneficiary located in a foreign country;
- Structured cash transactions through the use of multiple transactions at multiple branches of the financial institution where the account is maintained;
- Account holders using their personal accounts to act as possible agents of wire remitter businesses;
- Personal accounts used as “layering” points involving wire transfers sent into those accounts from unregistered and/or unlicensed MSBs and then transferred abroad;
- Cash intensive businesses (for example, restaurants) providing transfer services to groups of people by accepting cash to facilitate payments to customers’ family members residing in a foreign country;
- Businesses conducting structured cash deposits and drawing checks from their account to purchase bulk phone cards and/or stored value cards for possible resale;
- Similarly, a subject engaged in the suspected operation of an unlicensed MSB conducting numerous outgoing wire transmissions out of his personal account, in addition to drawing checks from his account to pay for phone cards;
- Use of possible shell companies and multiple accounts to facilitate the structuring of cash, deposit of money orders, and the negotiation of third party checks, followed by wire transfers from the accounts to high risk countries;
- Deposits of cash into accounts and subsequent outgoing overseas wire transfers by unregistered and/or unlicensed MSBs conducted on behalf of expatriate workers wishing to send money back home to their families; an account is typically maintained to service customers in one state or locale, while the actual account holder (or an agent) conducts the remittance transactions from another state. In one

reported instance, foreign cruise line employees transferred cash to an unlicensed MSB via an intermediary who carried the cash from the ship and deposited it into the unlicensed MSB account at a nearby bank branch on shore. The account holder was actually located several states away and transferred the funds to an associate in a foreign country for further dispersal to relatives of the cruise line employees, also residing in the foreign country.

Securities & Futures Industries SARs (SAR-SFs): The First Quarter

Brokers or dealers in securities, one segment of the securities and futures industries, were required to report suspicious financial activity beginning in January 2003. By mid-March, a total of 119 entities had filed 555 SAR-SFs. Statistical analysis of the SAR-SF data revealed several interesting trends and patterns.

Violations Types

The table below provides a breakdown of all the types of reported violations on FinCEN Form 101 submitted by the 119 entities. Note: The totals will exceed the number of SAR-SFs filed (555), because SAR-SFs can specify more than one type of suspicious activity per form.

Table 2: Breakdown of All the Types of Reported Violations on FinCEN Form 101

Types of Suspicious Activity Reported	SAR SFs	Percentage of Total SAR SFs Reviewed
Bribery/Gratuity	4	0.7
Check Fraud	112	20.2
Computer Intrusion	3	0.5
Credit/Debit Card Fraud	32	5.8
Embezzlement/Theft	74	13.3
Forgery	15	2.7
Identity Theft	86	15.5
Insider Trading	7	1.3
Mail Fraud	4	0.7
Market Manipulation	1	0.2
Money Laundering/Structuring	154	27.7

Prearranged or Other Non-Competitive Trading	2	0.4
Securities Fraud	10	1.8
Significant Wire or Other Transactions without Economic Purpose	56	10.1
Suspicious Documents or ID Presented	22	4.0
Terrorist Financing	2	0.4
Wash or Other Fictitious Trading	1	0.2
Wire Fraud	23	4.1
Other	157	28.3
None	8	1.4

Violation Amounts

Reported amounts in the 555 SAR-SFs submitted by broker-dealers ranged up to $5 billion. Twelve reported amounts of at least $100 million, including five filed in New York, three in San Francisco, three in Iowa, and one in Miami. Approximately 40 percent of the SAR-SFs reported amounts between $10,000 and $99,999.

Types of Instruments

Many types of financial instruments were involved in the suspicious activity reported on the SAR-SFs. The following table provides a breakdown of the instrument types. Note: The totals will exceed the number of SAR-SFs filed (555), because SAR-SFs can specify more than one type of financial instrument.

Table 3: Types of Financial Instruments

Types Of Financial Instruments Reported	SAR-SFs	Percentage of Total SAR-SFs Reviewed
Cash or Equivalent	276	49.7
Other	101	18.2
Money Market Mutual Fund	45	8.1
Stocks	37	6.7

None	35	6.3
Mutual Fund	33	5.9
Bonds/Notes	25	4.5
Other Non-Securities	13	2.3
Other Securities	6	1.1
Commercial Paper	1	0.2
Warrants	1	0.2
Foreign Currencies	1	0.2

Eighty included an additional instrument description. Of these, the most frequently mentioned were business or personal checks (39); wire transfers (12); counterfeit or stolen checks (9); cashier's or official checks (6); life insurance policies (6); brokerage accounts (5); and debit cards (5). One SAR specified "precious metals" under commodity type.

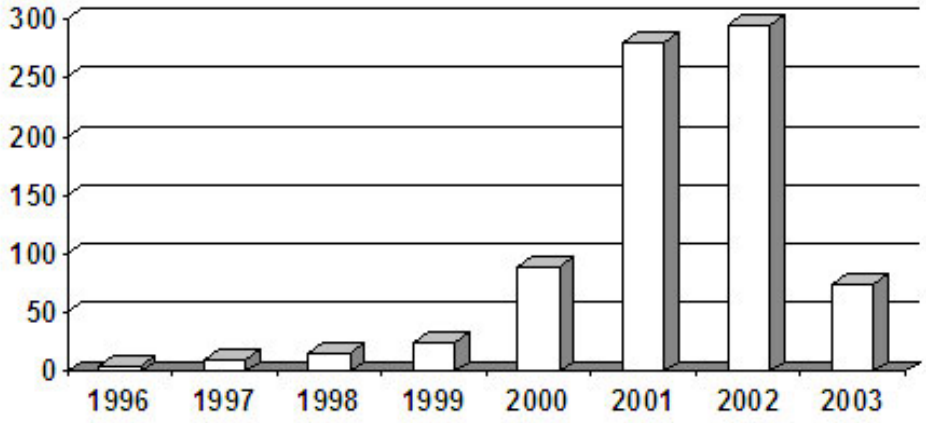
Online and/or Internet Banking

Recently, FinCEN conducted a study of SARs related to Internet and/or online banking. These SARs often used the terms, "online" and "Internet" interchangeably. For example, a bank may state that a customer conducted transactions via Internet banking, rather than specifying that the customer transacted through the bank's online facilities.

A search of the Suspicious Activity Reports Query System resulted in 776 "hits." The research was conducted for the period April 1, 1996 through April 18, 2003. As evidenced from the chart below, the volume of SAR filings that discuss online or Internet banking increased considerably. One reason for the increase may be the June 2000 addition of "Computer Intrusion" as a specific violation type on the depository institution SAR Form.

Chart 2: SARs "Hits"

April 1, 1996 thru April 18, 2003



Statistical Overview

A total of 291 separate financial institutions, including six foreign banks licensed to conduct business in the United States, filed 776 SARs between April 1996 and April 2003. The SARs were filed in 47 states, the District of Columbia and Puerto Rico. The five states with the most filings were: California (145 or 18.7 percent), Texas (80 or 10.3 percent), New York (55 or 7.1 percent), Florida (52 or 6.7 percent), and Ohio (30 or 3.9 percent). Those five states filed 362 or 46.6 percent of the SARs in this study.

The 776 SARs identified 983 violations. The most frequently cited violations were:

- Other—198 SARs or 20.1 percent;
- Check Fraud—190 SARs or 19.3 percent;
- Computer Intrusion—160 SARs or 16.3 percent;
- BSA/Structuring/Money Laundering—145 SARs or 14.8 percent;
- Counterfeit Check—78 SARs or 7.9 percent.

Violation amounts ranged up to $82.3 million. Twenty-two SARs exceeded $1 million.

One hundred twenty two separate bank branches in 31 states filed 126 SARs as a result of information received from their Internet Service Provides (ISPs). One bank headquartered on the West Coast filed 68 percent of the 100 BSA/Structuring/Money Laundering SARs. Almost all of those SARs reported structuring of cash deposits and withdrawals. The remaining 32 percent of the BSA/Structuring/Money Laundering SARs also reported primarily structured cash deposits. Frequent, sometimes more than one a day, cash deposits were made to an account followed by online transfers from the receiving account to another account (i.e., moving funds electronically from a checking account to a money market account or from a savings account to a business account). One SAR revealed cash deposits, followed by preauthorized online withdrawals by an international money transmitter.

SARs Filed by or About Internet Banks

Four Internet banks filed 17 SARs. At first glance, this may seem like a relatively small number of banks as well as SARs filed. However, only approximately 40 Internet banks operate in the United States, as opposed to 20,000+ brick-and-mortar banks and credit unions currently conducting business across the country. Financial institutions across the United States

detected that many transactions were conducted through Internet banks. Sixty-eight SARs mentioned this type of activity.

The common types of violations reported in SARs referencing Internet banks were:

- Check Fraud;
- Counterfeit Check;
- BSA/Structuring/Money Laundering;
- Identity Theft;
- Credit Card Fraud;
- Other: Unauthorized ACH Debits;
- Check Kiting.

Internet Gambling

The number of Internet gambling sites has increased substantially in recent years. In addition to on-line, casino-style gambling, there are numerous sport books taking bets on sporting events. Most of these websites are physically located in offshore jurisdiction. These operations accept bets and wagers from persons in the United States in violation of United States law, including 18 U.S.C. Section 1084, 1952, and 1955. For example, the majority shareholders of Gold Medal Sports Book, which was located in Curacao, N.V., pled guilty in federal court in Wisconsin to violating Section 1084 for accepting sports wagers from customers in the United States over the telephone lines and over the Internet. The company pled guilty to violations of the Racketeer Influenced and Corrupt Organizations (RICO) Act. In another example, the United States Attorney's Office in St. Louis reached a civil settlement agreement with a company called PayPal to settle allegations that PayPal aided in illegal offshore and on-line gambling activities. PayPal agreed to pay $10 million to the government to settle this claim.

In March 1999, a federal grand jury in Manhattan charged Jay Cohen with conspiracy to violate the Wire Wager Act, 18 U.S.C. Section 1084(a), and seven substantive counts of violating, and aiding and abetting violations of that Act, in connection with Cohen's operation of World Sports Exchange ("WSE"), a book making organization that Cohen owned and ran over the Internet from Antigua. The Wire Wager Act makes it unlawful to use a wire communication facility to transmit in interstate and foreign commerce to "bets or wagers" on sporting events, "information assisting in the placement" of any such bets or wagers, or a communication "which entitles the recipient to receive money or credit as a result of bets or wagers." Cohen was charged with violating all three clauses of Section 1084(a). After a two-week trial in February 2000, the jury convicted Cohen on all charges. In August 2000, Cohen was sentenced to 21 months' imprisonment. Cohen's conviction was affirmed and in June 2003, the United States Supreme Court refused Cohen's petition for review. In October 2002, Cohen began serving his sentence.

In January 2000, the U.S. Attorney's Office for the Eastern District of Missouri successfully prosecuted an offshore sports book operation based in Curacao, which took bets from U.S. citizens in violation of the Wire Wager Act. The individual defendants were charged with tax crimes as well as money laundering, and the Paradise Casino was charged with money laundering. This prosecution led to the forfeiture of millions of dollars of property derived from the proceeds of Wire Wages Act violations and resulted in Paradise Casino agreeing to pay over $11,000,000 in back excise taxes, interest and penalties based on violations of the Internal Revenue Code for failure to pay excise taxes on the gambling activity.

While many companies operate their games in an apparently fraud-free fashion, the potential for gaming fraud is greater via the Internet than in the physical realm. This is because start-up costs are relatively low and software is readily available. Similar to scam telemarketing operations, on-line gambling establishments appear and disappear with regularity, collecting from losers and not paying winners, and with little fear of being apprehended and prosecuted.

Internet gamblers operating offshore may be allowed to operate legally by the offshore jurisdiction in which they are physically located, but if they operate in whole or in part, virtually or physically in the United States, they are subject to prosecution under the Wire Wager Act if they take bets, transmit or receive betting information or transmit funds in support of unlawful activity, in accord with the Wire Transfer Act itself. While these Internet gambling operations may or may not be perpetrating a fraud on their customers, they could still be subject to prosecution under U.S. law for, among other things, violations of the Wire Wager Act, transmitting funds in violation of 18 U.S.C. 1960 or failing to pay excise taxes in violation of the Internal Revenue Service.

In addition to providing a venue for fraud and other elements of organized crime, Internet gaming offers considerable potential for money laundering. In the United States, land-based casinos are required to file suspicious activity reports and currency transaction reports with the Treasury Department's Financial Crimes Enforcement Network (FinCEN) and all financial institutions, which now by definition specifically include casinos, are required to adopt money laundering compliance programs.

While land-based casinos are known to be used in the placement stage of money laundering, in which currency is introduced into the financial system, Internet gambling is particularly well-suited for the laying and integration stages of money laundering, in which launderers attempt to disguise the nature or ownership of the proceeds by concealing or blending transactions within the mass of apparently legitimate transactions. Due in large measure to the volume and speed of transactions, as well as the virtual anonymity offered by the Internet, offshore gambling websites are an area of considerable money laundering concern. The Internet gambling operations are, in essence, the functional equivalent of wholly unregulated offshore banks with the bettor accounts serving as bank accounts for account holders who are, in the virtual world, virtually anonymous. For these reasons, Internet gambling operations are vulnerable to be used, not only for money laundering, but also for criminal activities ranging from terrorist financing to tax evasion.

The FATF's Report on Money Laundering Typologies 2000-2001 set forth scenarios involving money laundering in conjunction with Internet gambling. In a report published in February 2001, FATF noted that, "Internet gambling might be an ideal web-based 'service' to serve as a cover for a money laundering scheme through the net. There is evidence in some FATF jurisdictions that criminals are using the Internet gambling industry to commit crime and to launder the proceeds of crime." In June 2003, the Financial Action Task Force on Money Laundering (FATF), the leading multilateral international anti-money laundering organization, recognized the ever-increasing problem that Internet gambling represented and revised its forty anti-money laundering recommendations to include, among other things, recommendations affecting casinos and specifically including Internet casinos.

Trade-Based Money Laundering

Criminal individuals and organizations have long misused international trade mechanisms to avoid taxes, tariffs, and customs duties. As both the formal international financial system and money service businesses become increasingly regulated, scrutinized, and transparent, criminal money launderers and terrorist financiers are increasingly likely to use fraudulent trade-based practices in international commerce to launder, earn, move, and integrate funds

and assets. U.S. Customs officials define trade-based money laundering as the use of trade to legitimize, conceal, transfer, and convert large quantities of illicit cash into less conspicuous assets or commodities. In turn, the tangible assets or value are transferred worldwide without being subject to financial transparency laws and regulations.

Trade-based value transfer schemes use commerce in both licit and illicit goods to transfer value. Invoice fraud involving a shipment of trade goods from country A to country B provides a simple and effective way to launder the proceeds of criminal activity. For example, over-invoicing a shipment of goods gives criminal organizations a paper rationale to send payment abroad and/or to launder money. Thus, if a container of electronics is worth $50,000, but is over-invoiced for $100,000, the subsequent payment of $100,000 will cover both the legitimate cost of the merchandise ($50,000) and allow an extra $50,000 to be remitted or laundered abroad. The business transaction and documentation disguises the illicit transfer of $50,000, and washes the money clean.

There are a multitude of other types of invoice fraud and trade manipulation; for example, false invoicing, double invoicing, and drawback and carousel fraud. Drawback is the refund of customs duties, taxes or fees on goods destined for favored uses. Carousel fraud is the import, re-export, or diversion of goods that fraudulently obtain drawback, export subsidies and/or value added tax. For instance, export incentives often encourage and disguise fraud. In this scheme, a government pays cash incentives to a company to export products, and the company uses the same export to launder money. In some countries, traders report to exchange control authorities that imports cost more, or exports less, than the actual cost. The excess foreign exchange generated can be used to purchase additional foreign trade items. In some areas of the world, trade goods are simply bartered for other commodities of value. In regions of Pakistan and Afghanistan, illegal drugs are commonly thought of as a commodity or trade good. Law enforcement authorities have reported, for example, that the price for a kilogram of heroin in this region of the world is a color television set. There are other barter networks where narcotics in Pakistan and Afghanistan are exchanged for foodstuffs such as vegetable oils.

These simple schemes become more complex when the misuse of trade also involves traditional and entrenched ethnic-based trading networks, indigenous business practices, smuggling, corruption, narcotics trafficking, the need for foreign exchange, capital flight, terrorist financing and tax avoidance. Frequently, many of these illegal techniques are commingled and intertwined, making it extremely difficult for investigators to follow the trail and conduct effective law enforcement investigations.

There is a wide range of estimates on the total annual flow of transactions through informal banking systems. The United Nations estimates $200 billion, the World Bank and International Monetary Fund estimate tens of billions of dollars, and a FinCEN report noted that quantifying the amount with certainty is virtually impossible. If tax and duty evasion is included, the amount of money laundered worldwide through these trade-based systems is undoubtedly staggering. U.S. officials estimate that the United States government alone loses tens of billions of tax revenue every year due to artificial overpricing and under pricing of products entering and leaving the country. Because it allows them to shift profits abroad, criminal individuals, corporations and other enterprises engage in abnormal international trade pricing that transfers value and/or reduces U.S. tax liability. Recent examples of abnormally priced transactions include cotton dishtowels imported from Pakistan into the U.S. for the absurdly high price of $153.72 each, briefs and panties imported from Hungary for $739.25 a dozen, metal tweezers imported from Japan at $4,896 a unit, toilet bowls exported to Hong Kong for the ridiculously low price of $1.75 each, and missile and rocket launchers exported to Israel for a mere $52.03 each. Although transactions such as these can result in substantial loss of revenue for the governments involved, criminals also know that moving and laundering money by these very

simple techniques are virtually undetectable in the conduct of international trade.[1]

Trade and Terrorist Financing

Trade-based value transfer is prevalent in many parts of the world that are vulnerable to terrorist financing. At present, it is impossible for law enforcement and customs to interdict all suspect transactions in this underworld of trade. At times, however, trade-based systems intersect with banks and other traditional financial institutions, which allow terrorist financiers or money launderers to obtain currency needed to purchase goods for further fund transfer. Financial institutions can also serve terrorist financiers as links in a clearing process that involves wire transfers. Where trade-based money laundering/terrorist financing intersects with financial institutions, law enforcement must develop techniques to identify the brokers or their representatives. Moreover, at that point, financial institutions may then be able to review the trade-related financial transactions for indications of unusual activity, which may be reported to authorities in suspicious activity reports. The financial community, law enforcement, and customs officials must seek a more aggressive role in recognizing how trade can be used in money laundering and in the financing of terrorism so as to conduct effective law enforcement investigations.

In one example of how alert customs scrutiny stopped suspect trade goods with ties to terrorism, a European customs service intercepted a shipment of transshipped toiletries and cosmetics that originated in Dubai. Customs examination of the manifest suggested that the goods were counterfeit and they were grossly undervalued. The goods were ultimately consigned to a third country. The resultant investigation revealed that the original exporter of the goods was a member of al-Qaida.

Law enforcement sources reveal that al-Qaida, as well as its ally in Southwest Asia, Jemaah Islamiya, are also involved in international drug trafficking to help them buy arms and finance operations. When illegal drugs are used in barter transactions for goods or services, they serve as an underground currency for terrorism.

Alternative remittance systems, sometimes also known as informal value transfer systems (IVTS), parallel banking, or underground banking, move money or transfer value without necessarily using the regulated financial industry. Trade-based money laundering can also be viewed as a component of other types of alternative remittance systems, such as hawala, the Black Market Peso Exchange, and the misuse of precious metals and gems. Informal banking systems such as hawala are a very efficient and very effective method of moving money or transferring value. Generally, the transfer of funds between sender and receiver must be settled. This can be done via a variety of methods such as the physical movement of money, wire transfer or check, payment for goods to be traded, invoice manipulation, and the trade in precious metals and gems.[2] Historically and culturally, in all of these alternative systems, trade is the method of choice to provide “countervaluation” or a method of “balancing the books.”

[1]November 2002 press release by Florida International University finance professor John Zdanowicz PHD and Penn State University finance professor Simon Pak, Ph.D.

[2]All of these systems have been reported upon in depth in previous editions of the International Narcotics Control Strategy Report.

The September 11, 2001 terrorism attacks prompted U.S. law enforcement authorities to focus greater attention on the possibility that terrorist financing takes place through informal banking systems such as hawala. Yet according to the FBI, some of the September 11 hijackers allegedly used hawala to transfer thousands of dollars in and out of the United States prior to their attacks. In addition, Somalis working in the United States used the Al Barakaat informal banking network to send money to their families in Somalia. Al Barakaat was founded with

significant investment from Usama bin Laden. Al Barakaat's worldwide network was reportedly also channeling several million dollars a year to and from al-Qaida.

It is readily apparent that criminal organizations the world over use value transfer and asset concealment systems that are culturally indigenous and avoid government scrutiny. Recent reports indicate that terrorist organizations increasingly use cash or have shifted resources into assets such as gold and diamonds and other untraceable commodities to avoid financial institutions' transparency networks. According to a September 2002 United Nations Security Council letter, al-Qaida was believed to have converted some of its assets into gold and diamonds. According to Global Witness, a nongovernmental organization, British forces in Afghanistan found an al-Qaida training manual that describes techniques for the smuggling of gold. Press reporting has detailed the use of gold, diamonds, tanzanite and other precious commodities by terrorist groups.[1]

[1]The reference above to al-Qaida and to the UN letter are noted in the GAO Report to Congress on "Terrorist Financing-U.S. Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms," November, 2003.

Black Market Peso Exchange—Trade and the Underground Economy

One of the most prevalent methods of laundering money through trade in the Western Hemisphere is via the Colombian Black Market Peso Exchange or BMPE. This money laundering technique is used by Colombian drug trafficking organizations to convert U.S. drug dollars in the U.S. to Colombian pesos in Colombia without the inherent risk of smuggling the bulk currency across international borders. The placement stage of this money laundering technique frequently involves the evasion of U.S. Bank Secrecy Act reporting requirements.

In simple terms, Colombian cartels sell drug-related, U.S. dollars to black market peso exchangers in Colombia. Once this currency exchange has occurred, the trafficking organization has effectively laundered its money and is out of the BMPE process. The peso broker, on the other hand, must then launder the accumulated U.S. dollars in the United States. The peso broker uses a variety of methods to place the U.S. narcotics proceeds into financial institutions. (For U.S. law enforcement, the "placement" stage in money laundering represents the best opportunity to identify and interdict money laundering.) The peso broker, operating in Colombia, thus has a pool of narcotics-derived funds in the United States to "sell" or "exchange" to legitimate Colombian importers. The funds are used to purchase trade goods such as cigarettes, electronics, and gold.

The U.S. Department of Treasury's Internal Revenue Service Criminal Investigation Division (CID) has an Illegal Source Financial Crimes Program that recognizes that money gained through illegal sources is part of the untaxed underground economy. The underground economy is a threat to the U.S. voluntary tax compliance system and undermines the overall public confidence in the tax system. The Internal Revenue Code generally states that all income is taxable, from whatever source it is derived. The IRS Narcotics Related Financial Crimes Program seeks to reduce the profits and financial gains of narcotics trafficking and money laundering organizations that comprise a significant portion of the untaxed underground economy. In the case of BMPE investigations, the IRS and other law enforcement agencies, such as the Immigration and Customs Enforcement Agency and the Drug Enforcement Administration, seek to disrupt a trade-based money laundering methodology that aims to legitimize the proceeds of narcotics trafficking by exchanging funds for trade items often found in the untaxed underground economy. U.S. and Colombian law enforcement and regulatory officials are continuing to cooperatively seek system-wide solutions to this problem that would break the importers' reliance on drug dollars to pay their international debts.

2003