The SAR Activity Review

Trends Tips & Issues

Issue 6

November 2003

The SAR Activity Review

Trends

Tips &

Issues

Issue 6

Published under the auspices of the Bank Secrecy Act Advisory Group

November 2003

Table of Contents

Introduction

The SAR Activity Review-Trends, Tips and Issues is a product of continuing dialogue and close collaboration among the nation's financial institutions, law enforcement officials, and regulatory agencies[1] to provide meaningful information about the preparation, use, and value of suspicious activity reports (SARs) filed by financial institutions.

This edition, Issue 6, reflects the continuing maturation and expansion of the SAR process itself. Depository institutions are substantively improving the quality of their SAR reporting; SARs are capturing more criminal activity as the reporting requirements expand to additional financial industry sectors, and law enforcement is successfully investigating and prosecuting more SAR-enhanced cases. These efforts are resulting in better feedback to the industry so that it can contribute to enhanced SAR reporting—a primary objective of the FinCEN network.

To better present this dynamic expansion, Issue 6 introduces a new delivery format. The statistical data, formerly found in Section One, Suspicious Activity Report Statistics, and in the Appendix 1, Characterization of Suspicious Activity by States and Territories by Year, now appears in a companion product entitled *The SAR Activity Review–By the Numbers*. The first edition of that report was produced recently and is available on the FinCEN website, www.fincen.gov. Future editions of *By the Numbers* will be produced semiannually to cover two filing periods: January 1 to June 30 and July 1 to December 31. All editions will be available on the FinCEN website following the end of each period, in the early spring and early fall of each year. *By the Numbers* will be presented in an Excel format to allow readers to download and manipulate the information to achieve maximum management and compliance needs for their institution or agency.

All of the other sections formerly published in *The SAR Activity Review-Trends, Tips and Issues* will be published semiannually in the spring and fall. These new

---

[1] These include, among others, the American Bankers Association; Independent Community Bankers of America; American Institute of Certified Public Accountants; Securities Industry Association; Futures Industry Association; Non-Bank Funds Transmitters Group; Federal Reserve Board (FRB); Office of the Comptroller of the Currency (OCC); Federal Deposit Insurance Corporation (FDIC); Office of Thrift Supervision (OTS); National Credit Union Administration (NCUA); U.S. Securities and Exchange Commission (SEC); U.S. Department of Justice's Criminal Division and Asset Forfeiture & Money Laundering Section and the Federal Bureau of Investigation (FBI); U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement (ICE) and U.S. Secret Service (USSS); U.S. Department of the Treasury's Executive Office of Terrorism Financing and Financial Crime (EOTF/FC), Internal Revenue Service (IRS), and the Financial Crimes Enforcement Network (FinCEN).

issues, and previous issues of *Trends, Tips and Issues* dated October 2000, June 2001, October 2001, August 2002, and February 2003, will continue to be available through FinCEN's website and in hardcopy form. Analytic reports, issue papers, and other publications related to or resulting from information contained in *The SAR Activity Review* may be published separately.

Significant topics presented in Section 1 of this issue include the identification of potential money laundering and terrorist financing methods involving monetary instruments that clear through the cash letter process, potential terrorist financing methods that can occur through coupon redemption fraud schemes, and an update of findings related to terrorism, terrorist financing, and informal value transfer systems (IVTS). In Section 2, SAR analysis is provided on broker-dealers in securities—one of the newer industries now under mandatory SAR reporting. Also included is information about on-line banking and the real estate industry. Section 3 provides summaries of the use of SAR filings in criminal investigations, and Sections 4 and 5 provide important information to improve the quality of SAR Reporting. Section 6 is a news update on various related activities affecting the SAR program. Section 7 provides insights from one of our industry partners, and Section 8 introduces the new Feedback Form. Our new Appendix section provides a listing of current and previous *SAR Activity Review* topics with the FinCEN website hyperlink to the specific editions. Throughout this issue, readers will find announcements about special Advisories and Bulletins related to emerging money laundering and terrorist financing threats and issues, which FinCEN recently published or is about to publish.

Your comments and feedback are important to us. Please take a moment and let us know if the topics chosen are helpful and if our new publication process is beneficial. We have included a feedback sheet in Section 8. Your comments may be addressed to either or both of *The SAR Activity Review* project co-chairs:

John J. Byrne
Senior Counsel and
Compliance Manager
American Bankers Association
1120 Connecticut Ave., NW
Washington, DC 20036
(202) 663-5029 (phone)
(202) 828-5052 (fax)
jbyrne@aba.com

David K. Gilles
Assistant Director
Office of Strategic Analysis
Financial Crimes Enforcement
Network (FinCEN)
(703) 905-3574 (phone)
(703) 905-3698 (fax)
gilled@fincen.treas.gov

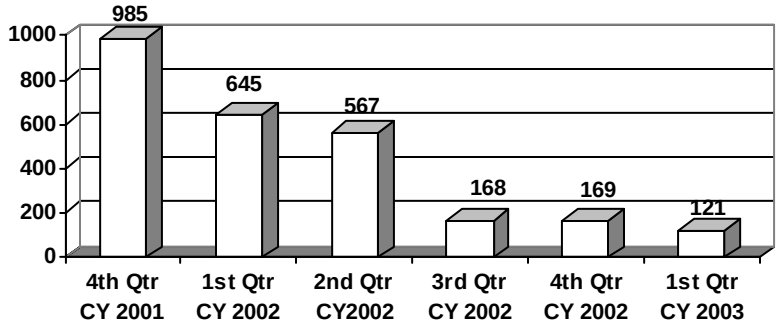
Section 1 - Trends and Analysis

Terrorism and Terrorist Financing

The purpose of this Section is to provide financial institutions with information relative to various aspects of terrorist financing to assist them in identifying and reporting related suspicious activity. Issues 4 and 5 of *The SAR Activity Review*, SAR Bulletin Issue 4—The Aspects of Financial Transactions Indicative of Terrorist Funding, and FinCEN Advisory Issue 33— Informal Value Transfer Systems (IVTS) discussed the vulnerabilities of a financial system to terrorist financing. The last two editions of *The SAR Activity Review* provided statistical data and information concerning terrorist-related SARs.

FinCEN has continued 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 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 (OFAC) or other watch lists] or 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 suspicious activity as being potentially terrorist-related on their own. This section will offer a synopsis of SAR statistical data for the recent review period and will identify the general types of activities being reported in terrorist-related SARs.

The following chart represents SARs filed relating to terrorism for the 18-month period (by CY quarters), commencing October 1, 2001 and ending March 31, 2003.



As shown in the above chart, 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 on the World Trade Center, the Pentagon, and over Somerset County, Pennsylvania.

Listed below 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% 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 from $0 to $193 million.

- Financial institutions indicated that 68 SARs (23.4%) were reported directly to law enforcement. (Box 40 was checked on the SAR.)[2]

Eighty-four SARs (29%) 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. Four SARs make direct mention of compliance with Section 314(a).

The activity described in the SARs remained consistent with the activity described in *The SAR Activity Review*, Issue 4 (August 2002) and Issue 5 (February 2003). The activity included wire transfers predominantly to and from Middle Eastern

[2] In situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, financial institutions shall immediately notify, by telephone, appropriate law enforcement and financial institution supervisory authorities in addition to filing a timely SAR to the Detroit Computing Center. Institutions are also encouraged to use the Financial Institutions Hotline (1-866-556-3974) established by FinCEN in October 2001 for the purpose of expediting voluntary reports to law enforcement of suspicious transactions that may relate to terrorist activity.

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%) 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 institutions 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% to 80% were filed based on government watch lists, while 20% to 25% were filed at the depository institutions' initiative. According to information in the SARs reviewed, several depository institutions have established internal watch lists that alert tellers and other employees of previous suspicious behavior by customers.

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.

Informal Value Transfer Systems (IVTS)

In March 2003, FinCEN issued Advisory 33,[3] which provided a general overview of informal value transfer systems (IVTS) and indicators of such activity. As part of the Advisory, FinCEN provided instructions to financial institutions regarding the filing of IVTS-related SARs. The guidance instructed depository institutions to check the "Other" box in Part III, Line 35(s) on Form TD F 90-22.47 and note the abbreviation "IVTS" in the space following the box in instances where the financial institution had reason to believe the activity to be IVTS-related. Some financial institutions have followed that guidance and, in doing so, have provided valuable and more easily retrievable information to FinCEN and law enforcement regarding IVTS trends and patterns. Depository institutions should continue to follow the guidance in Advisory 33 for reporting IVTS-related suspicious transactions. Filers of Form TD F 90-22.56 (Suspicious Activity Report by Money Services Business), FinCEN Form 101 (Suspicious Activity Report by the Securities and Futures Industries), and FinCEN Form 102 (Suspicious Activity Report by Casinos and Card Clubs) should also follow these instructions when completing those forms.

Parallel to the release of Advisory 33, FinCEN completed an analysis of a sampling of SARs referencing IVTS or IVTS-like operations. Four predominate themes identified from those SARs are:

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

Examples of the types of activities reported by institutions related to these themes may be found in the remainder of this section.

Illegal Money Transmitter Businesses

Forty-five SARs (or 56.3 %) filed regarding unregistered and/or unlicensed money transmitter businesses identified a variety of techniques commonly used by IVTS operators to facilitate the transfer of funds on behalf of their customers. Many unlicensed/unregistered money transmitters were identified by the filing institution

[3] See FinCEN Advisory Number 33, Informal Value Transfer Systems, at http://www.fincen.gov/pub_main.html. Also refer to Issue 5, page 17, of *The SAR Activity Review – Trends, Tips & Issues*, published by FinCEN in February 2003.

as IVTS 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 IVTS operations are considered money services businesses (MSBs) by virtue of the funds/value transfer services they provide to their customers. Financial institutions often identify IVTS operations when exercising effective due diligence on customers who claim to be money remitters yet fail to provide adequate proof that the business is registered with the Department of the Treasury or appropriately licensed in respective states where such licenses are required. 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 IVTS services. The SARs analyzed for this study provided a number of such indicators:

- Use of personal accounts to facilitate the negotiation of cash and third-party checks followed by outgoing wire transfers;
- 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;
- Structured cash transactions through the use of multiple transactors at multiple branches of the financial institution where the suspect 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.

- Multiple wire transfers sent from unregistered and/or unlicensed MSBs to benefit a single beneficiary located in a foreign country; and

- Unlicensed and/or unregistered MSBs sending large volumes of wire transfers to a single personal account within the United States; transactors in multiple states conduct cash deposits into the same personal account.

Hawala and Other IVTS

FinCEN identified 19 SARs (or 23.8 %) filed by financial institutions referencing hawala and/or broadly indicating other facets of IVTS. The term “hawala” simply

means transfer in Arabic and is commonly associated with IVTS activities that occur in southwest Asia and the Middle East. Since the tragic events of September 11th, the financial community has acquired a better understanding of hawala and other IVTS(s) located in the United States and throughout the world, as well as observing their nexus with bank accounts.

The following extracts were taken from SARs associated with hawala and similar types of IVTS-related activity:

- A wire transfer company was identified as a hawala by the filing financial institution. The company sent a large volume of wire transfers to an Arabian Gulf nation.

- A financial institution identified a customer who accepted large volumes of money orders and other monetary instruments deposited into his personal account. When questioned about the activity, the customer indicated he provided services, through his brother residing in a south Asian country, to local expatriates wishing to send merchandise to their families in their home country. The customer further indicated he accepted payment from his customers either by money order or cashier's check. When his customers provided these payments, the suspect customer contacted his brother to release the merchandise to the particular family member abroad.

- A former banking employee was suspected of acting as an unlicensed money transmitter on behalf of his brother located in a West African nation. He would collect cash from local members of the community that would be deposited into his personal account, followed by wire transfers to trading companies in Asia and North America.

- An account held by a clothing and jewelry store was identified with large cash deposits and numerous deposits of checks and other monetary instruments. Once a month, a large wire transfer from the account was sent to a Southeast Asian country. [4]

- Street vendors, all expatriates of a south Asian country, deposited cash into accounts, from which the balances were subsequently wire transferred to a businessman residing in the south Asian country. When further questioned, the street vendors indicated they were conducting this

[4] The SAR author stated that she identified this activity based on her review of FinCEN Advisory Issue 33, Informal Value Transfer Systems, http://www.fincen.gov/advis33.pdf.

operation because only certain individuals could maintain accounts in the receiving country.

- An unregistered and/or unlicensed entity was identified as making several large cash deposits into its account, in addition to negotiating several checks drawn on personal accounts from all over the country. The funds were further transferred to a trading company located in an Arabian Gulf country.

- Two "students" were identified as the joint holders of a checking account. Several checks issued from a number of Arabian Gulf nations, including cultural offices, were deposited into the account. Checks were also drawn on the account made payable to other subjects, as well as other varied types of debit activity occurring through the account.

- A money exchange entity was identified as structuring over $3 million into an account within a one-month period. The account was set up to allow members of a local ethnic community to send funds to their families in a Southeast Asian country.

- Two SARs, filed on the SAR-MSB form, mentioned "hawala" in the narrative. The SARs identified a customer who visited multiple branches of the same money transmitter service to send funds to a south Asian country. Each transaction was under $3,000 and was forwarded to the same payee on multiple days.

Black Market Peso Exchange (BMPE)

Six SARs (or 7.5 %) were filed on suspected BMPE operations.[5] Some of the SARs highlighted emerging techniques possibly employed by BMPE operators to move cash to Colombia through the use of ATMs. In addition, traditional BMPE was also highlighted.

The type of activities revealed in these SARs include the following:

---

[5] See FinCEN Advisory Issue 12, Black Market Peso Exchange Update, issued June 1999, (http://www.fincen.gov/advis12.pdf) and FinCEN Advisory Issue 9, Black Market Peso Exchange, issued November 1997, (http://www.fincen.gov/advisu9.pdf) for additional background information pertaining to BMPE.

- Several accounts maintained at a financial institution were used to deposit bulk cash through domestic ATM transactions. Shortly after the deposits, numerous cash withdrawals of the funds were initiated via ATMs in Colombia.

- An account holder engaged in agricultural activity was identified as remitting a total of $400,000 to numerous financial institutions located in Central America. The subject was suspected by the filing bank as engaging in possible BMPE operations based on secondary information received by the financial institution.

International Emergency Economic Powers Act (IEEPA) Violations

Financial institutions filed ten SARs (or 12.5%) regarding the attempted violation of IEEPA regulations.[6] The detection of these violations occurred when subjects attempted to transfer funds to OFAC-blocked countries through a U.S. financial institution. In most cases, existing anti-money laundering programs and effective due diligence of financial transfer requests prohibited the initiation of transfers.

Examples of some of these filings are listed below.

- A SAR was filed on an unlicensed and/or unregistered MSB that provided remittance services to an OFAC-blocked country located in the vicinity of the Arabian Gulf. During the course of several years, numerous individuals, not associated with the account, used one personal account to facilitate deposits in various states. Funds were then either converted to a cashier's check or wired abroad. Funds were transferred to the benefit of one family in an OFAC-blocked country through agents of the remitter organization residing in neighboring countries.

- A suspect attempted to cash a $60,000 check at a local financial institution and inquired about how thick the money would be because she was going to mail it. Previously, the customer had attempted to send a wire transfer from the bank to an OFAC-blocked country.

---

[6] For information about IEEPA and other OFAC-related regulations, visit the OFAC website at http://www.treas.gov/offices/eotffc/ofac/regulations.

- A customer believed to be engaged in the construction business in an OFAC- blocked country sent numerous wire transfers from a domestic-based account maintained by an associated apartment leasing and investment company. Rent checks were also deposited into this account. The financial institution believed many of the funds were sent to the OFAC-blocked country via a European bank, as well as through the suspect's use of money remitters and other companies.

SAR Filers Identify Suspicious Monetary Instruments Clearing Through International Cash Letters

International cash letter processing through correspondent accounts is a standard banking service provided by some U.S. financial institutions to foreign financial institutions.[7] In basic terms, an international cash letter is an inter-bank transmittal letter that accompanies checks or monetary instruments (such as money orders) sent from one bank to another internationally. Some banks that monitor their cash letter processes for suspicious activities have identified bulk movements of monetary instruments, which appear to be indicative of money laundering. Their observations are consistent with several recent law enforcement cases involving money laundering through bulk monetary instrument transactions. FinCEN is monitoring this reported activity to determine if it is indicative of a trend.

Investigations and SARs filed by financial institutions have revealed that monetary instruments, purchased in bulk with illicit proceeds, are sometimes cleared through cash letters. It is important to note that the clearing banks are several steps removed from the actual conversion of the illicit funds to monetary instruments. Their ability to nonetheless identify the indicia of suspicious activity in

[7] In basic terms, an "international cash letter" functions as a method of inter-bank communication for processing transactions between banks located in different countries. The communication is in the form of a document (cash letter) that accompanies checks, drafts, money orders, and traveler's checks. When submitted for collection by a foreign correspondent depository bank to the U.S. clearing bank, the cash letter details the number of checks or other items sent as well as the total dollar amount of the included items. Upon receipt from a foreign correspondent bank, the U.S. clearing bank sends the monetary instruments for clearance or negotiation to the financial institution(s) upon which the individual items were originally drawn. The foreign bank's account at the U.S. clearing bank will then be credited for the total amount of the cash letter.

the course of clearing these instruments suggests there may be a vulnerability at the stage at which the instruments are actually issued (for example, sequentially numbered monetary instruments endorsed by the same person aggregating to a high value). Thus, monitoring of the cash letter process can yield important insights into not only trends in bulk movement of monetary instruments but also potential vulnerabilities at their point of sale.

Fortunately, both regulatory authorities and the financial industry are becoming aware of these issues. The banking regulatory agencies have examination procedures requiring financial institutions to give enhanced scrutiny to cash letter processing, which has resulted in SAR filings. FinCEN's comprehensive study of IVTS[8] provided examples of suspicious activity involving the international transport of monetary instruments. For example, BMPE schemes reveal narcotic proceeds clearing through correspondent accounts via checks, money orders, and other types of monetary instruments. FinCEN has found the SARs filed by financial institutions from their monitoring of cash letters to be valuable in identifying such activity.

To further assist industry, FinCEN is currently conducting a comprehensive study of SARs that relate or refer to monetary instruments clearing through the international cash letter process. The findings of this study will report on any patterns and trends, as well as red flags that may be shared. It is envisioned that the issues raised from this ongoing research will stimulate further productive discussion among the law enforcement, regulatory, and financial communities.

Following are some examples of activities involving bulk monetary instruments and cash letters:

- In a case involving the Kumar hawala, the United States Attorney for the Eastern District of New York recently charged nine defendants with participating in the Kumar Organization's unlicensed money transmitting business. Kumar transmitted in excess of $32 million out of the United States between January 2001 and May 2003. The government alleged that in addition to illegal money transmissions, Kumar converted currency into

[8] See FinCEN's study entitled "A Report to Congress in Accordance with Section 359 of the USA PATRIOT Act, November 2002"; available on FinCEN's website www.fincen.gov

monetary instruments, including money orders and checks, and sent these funds via courier service outside the United States. On a single day, May 25, 2002, Customs Inspectors at Newark/Liberty International Airport intercepted Kumar's courier packages destined for Canada containing approximately $100,000.

- Law enforcement agents in the San Francisco area report that lower volume hawalas, particularly, are sending money orders overseas for negotiation.

- Law enforcement personnel at several major airports on the east coast have discovered large amounts of money orders in even amounts, and sequentially numbered, being sent regularly to a country in the Middle East.

Coupon Redemption Fraud

In the United States, hundreds of public and private corporations and manufacturers offer coupon discounts for products sold in retail stores. Coupons are found in newspaper inserts, magazines, mail solicitations, school and charity fund-raising booklets, in store aisles, and through Internet sites. According to NCH Marketing Services, which claims to be the largest clearing and processing agent for retailers and manufacturers worldwide, the total number of manufacturers' coupons printed and distributed in 2001 was 239 billion.[9] Legitimate coupon redemption generates billions of dollars in transactions each year. There is also the potential for criminals to abuse the coupon redemption system.

In February 2003, the United States Attorney for the Eastern District of Wisconsin and law enforcement officials with the FBI, United States Postal Service and the former U.S. Immigration and Naturalization Service[10] announced the indictment and arrests in five states of 16 individuals allegedly involved in a coupon redemption fraud and money laundering scheme that resulted in losses exceeding $4 million. According to the announcement, some of the proceeds were sent to the

[9] NCH Marketing Services press release, dated March 15, 2002.

[10] In March 2003, the Immigration and Naturalization Service (INS) transitioned from the Department of Justice to the Department of Homeland Security. Immigration enforcement services are now the responsibility of the Bureau of Immigration and Customs Enforcement (ICE).

West Bank and Jordan. The FBI is continuing to investigate the overseas financial transactions and other aspects of the scheme.[11]

As a result of this announcement, as well as testimony presented before the House Financial Services Oversight and Investigation Subcommittee in March 2003 concerning the possible nexus between the crime of coupon redemption fraud and the movement of the illicit funds to countries where terrorist organizations operate,[12] FinCEN reviewed SARs submitted from financial institutions related to coupon redemption fraud.

A search of the SAR database (April 1996 to present) revealed only two SARs related to activity described as coupon redemption fraud.[13]

- In 1998, a bank submitted a SAR to report the deposit of a $14,290 counterfeit check drawn on an account for a national coupon redemption service. Check Fraud was listed as the violation.

- In June 2002, a large depository institution located in several northeastern states submitted a SAR to report frequent deposits of large, even dollar checks issued by a coupon redemption clearinghouse and frequent, large, incoming wire transfers from the same originator, totaling $297,200. The funds were credited to a personal checking account at the bank. All checks and wires originated from an account held by the coupon redemption clearinghouse at another financial institution which was located in the same general area of the United States. The reporting bank had filed three previous SARs for structured cash deposits into the same personal account and a business account for the suspect. The June 2002 SAR listed the violation as BSA/Structuring/Money Laundering.

To better assist financial institutions in identifying suspicious activity related to coupon redemption fraud, the following information is being provided:

- A description of a legitimate coupon redemption process;

---

[11] News Summary release from the U.S. Department of Justice, United States Attorney, Eastern District of Wisconsin, dated February 26, 2003.

[12] Testimony before the House Committee on Financial Services Subcommittee on Oversight and Investigations Hearing on "Progress Since 9/11: The Effectiveness of U.S. Anti-terrorist Financing Efforts," March 11, 2003.

[13] Three SARs were identified during the search of "coupon fraud" but the SARs reported food coupon fraud, commonly called food stamp fraud, a type of criminal activity separate from coupon redemption fraud.

- A description of the activity associated with coupon redemption fraud; and

- Examples of the types of financial transactions which may be related to coupon redemption fraud schemes.

The information about legitimate and illegal methods stem from various case studies, industry information, and from Congressional testimony in March 2003 and earlier, during a hearing on "Foreign Terrorists in America: Five Years after the World Trade Center."[14] That testimony related the planners of the 1993 terrorist attack in New York to persons involved in coupon redemption fraud.

Legitimate Retail Coupon Redemption Process

The coupon is considered a legal obligation, an offer to consumers which contains written terms stating the specific discount when a particular product is purchased within a prescribed time frame. A legitimate retailer understands that a consumer must purchase a product at the time the coupon is accepted and before the coupon is submitted to a coupon clearinghouse for reimbursement.

A retail coupon clearinghouse is a business engaged by retailers to sort coupons on behalf of various manufacturers. The clearinghouse pays the retailer, minus a handling fee, for the coupon's value. The manufacturer or its agent pays the clearinghouse when it submits the coupons for redemption.

The legitimate process involves the following four steps:

Step 1: Registration

The owner of a store (e.g., grocery, pharmacy, convenience store, etc.) registers with a retail coupon clearinghouse by filing a registration form to accept coupons from consumers. The clearinghouse verifies that the store actually exists. The clearinghouse establishes an account for the store in order to track coupon submissions and make payments to the store.

---

[14] "Consumer Coupon Networks in the United States – the Terror Connection" presented by Ben Jacobson before the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information, February 24, 1998.

Step 2: The Store

The store accepts coupons from their consumers for products legitimately sold at the store. The store owner mails or ships bundled coupons to the clearinghouse for processing and to receive credit for the coupons submitted.

Step 3: The Coupon Clearinghouse

Coupon clearinghouse employees receive, count and sort coupons by manufacturer. (Note: Some clearinghouses do not immediately sort the coupons, using instead a weight-value formula to expedite payment to the retailer. Later, when the shipment is counted and audited, an adjustment, if needed, will occur.) The store's account is credited for the value of coupons submitted, minus a small handling fee. The clearinghouse redeems the value of the coupons from the manufacturers offering the products. A check payable to the store, in the amount of the total coupon value, is generated and sent to the store.

Step 4: Back at the Store

The business owner receives the coupon redemption check from the coupon clearinghouse. The coupon redemption check is deposited to the store's business account at the local bank.

Illegal Coupon Redemption Process

Some of the same steps found in the legitimate redemption process are incorporated into the illegal scheme. However, as with most criminal ventures, additional steps are found.

Step 1: Recruitment

- The criminal organization recruits willing business owners of generally small, independent convenience stores or neighborhood food stores by offering kickback payments to participate and act as a front in the scam.

- The organization may fabricate the existence of stores to claim that they accept coupons.

- If the crime is committed by a terrorist organization, business owners sympathetic to the organization's cause may volunteer their participation in the scheme.

- The business owners never see the actual coupons, only the redemption checks.

- The participating business owner registers with the coupon clearinghouse, allegedly to accept coupons from customers to send to the clearinghouse (in fact, if a store exists, the owner may accept legitimate coupons during the course of his regular operations.)

Step 2: Obtaining Coupons

- Members of the organization purchase bulk coupon inserts from recyclers, newspaper distributors, or small newspaper stands which sell Sunday papers.

- Some participating stores that sell newspapers remove coupon inserts from newspapers before they are displayed for sale. The inserts are supplied directly to the organization.

- Members purchase bulk coupon certificate booklets, normally sold for fundraising by schools and other legitimate organizations, to access and use the grocery coupons normally included in the booklets.

- Organizations use "dumpster divers" to sift through recycling bins and curb recycling containers to locate and remove coupon inserts from newspapers and magazines.

Step 3: Coupon Clipping Houses

- The organization staffs coupon-cutting locations (commonly referred to as "clipping houses") with employees who may or may not be aware of their participation in fraudulent activities; i.e., housewives or students who are recruited through legitimate-appearing advertisements to work part-time; the organization advertises for and uses home-based businesses.

- Clippers cut out the coupons from various mediums, and then wrinkle the coupons to appear aged or worn (as if they have been carried around by a consumer for a while.)

- The coupons are then sorted by product and grouped for shipping to a coupon clearinghouse. The address, shipping information, and account number is provided for the real or fabricated store participating in the scheme.

- The packaged, bulk coupons are shipped to targeted coupon clearing houses, frequently by courier rather than through the U.S. mail to avoid Federal mail fraud statutes if the scam is discovered.

Step 4: The Coupon Clearinghouse

- Upon receipt of the packaged, bulk coupons, clearinghouse employees sort the coupons and credit the submitting store's in-house account for the face value of the coupon submissions.

- The clearinghouse redeems the value of the coupons from manufacturers offering the products.

- The clearinghouse sends an audit payment in the form of a check, payable to the store or possibly to the business owner, to the store that claimed to have honored the coupons.

- The criminal organization may bribe a clearinghouse employee or place an operative inside the clearinghouse to review and approve fictitious registration applications.

Step 5: The Store Owner

- The business owner or an employee deposits the coupon redemption checks into the store's business account or to the owner's personal account at a financial institution.

- Subsequently, the owner withdraws the funds in the amount of the redemption checks as cash or uses the funds to purchase monetary instruments, such as money orders, cashiers checks, etc. The cash or monetary instruments are delivered to the criminal or terrorist organization, where the owner is paid for his services.

- In a different method, the business owner may hold the coupon redemption checks for delivery directly to members of the criminal or terrorist organization. Middlemen, sometimes called runners, employed by the organization, may visit participating stores to secure the redemption checks and give the business owner his cut. The checks are subsequently negotiated at

a licensed or unlicensed money services business for cash; used to purchase money orders; or transmitted by wire, domestically or out of the country.

Indicators of Suspicious Transactions in Coupon Redemption Fraud

While the vast majority of all financial transactions related to the coupon redemption process are legitimate and conducted in the normal course of business, criminals or terrorists have used the process for illicit gains, to launder money, or to possibly fund terrorist activity.

The following financial activities may be suspicious and indicate misuse of the coupon redemption process:

Depository Institution Transactions

- Frequent deposits to a business or personal account consist of one or more large, possibly even-dollar checks issued from coupon clearinghouses—specifically checks issued to businesses whose size, location, or clientele base may not support the frequency or amount of the checks. The deposits are followed by an immediate withdrawal of the exact or similar funds in cash; funds are used to purchase monetary instruments (e.g. official bank or cashiers checks, money orders or traveler's checks); or funds are used to send wire transfers to other domestic or foreign financial institutions. The amount of the deposit and the outgoing funds may not be exact since the business owner deducts his "cut" for participation in the scheme. (Note: The currency withdrawals might be structured to evade the currency reporting requirements of the BSA.)

- Similarly, deposits of one or more checks from coupon clearinghouses are made to business or personal accounts, followed by the immediate issuance of checks from the same account in the exact or similar amounts, payable to unknown individuals or businesses. The cycle is constant, with outgoing checks issued consistently to the same payees.

- A business owner frequently cashes checks, payable to the business or the owner, which are issued from coupon clearinghouses. The funds are taken as cash, used to purchase monetary instruments, or used to send wire transfers.

- A business owner, accompanied by one or more unidentified individuals, conducts transactions mentioned previously. The financial institution employees observe the owner presenting cash or the monetary instruments to the individuals.

- Frequent incoming large dollar wire transfers are sent from coupon clearinghouses to credit a small retail store's business account or the personal account of the business' owner. The store size, clientele size, and/or store location is not consistent with the volume of wires received from the clearinghouse.

Money Services Business (MSB) Transactions

- Coupon redemption checks in large, possibly even-dollar amounts, are cashed by individuals other than the payee (perhaps a business or another individual). The funds are disbursed as cash. The same individual negotiates the checks during daily or frequent visits to the MSB.

- Funds from the cashing of coupon clearinghouse checks are used to purchase money orders or to send money transmittals to financial institutions, other MSBs, hawalas, or other IVTS locations.

What to do

A financial institution that knows or suspects that a customer is conducting transactions that involve proceeds from coupon redemption fraud should file a SAR. The "Other" box in Part III, Line 35(s) on Form TD F 90-22.47 should be marked and "suspected coupon redemption fraud" should be noted in the space following the box. The narrative should also include an explanation why the depository institution suspects or has reason to suspect that the customer is involved in coupon redemption fraud. Other types of financial institutions required to file SARs should mark the "Other" box in the "Type of Suspicious Activity" section on their appropriate SAR form, note "suspected coupon redemption fraud" in the space following the "Other" box, and provide an explanation why the institution suspects or has reason to suspect the customer is involved in coupon redemption fraud.

Section 2 - Other Analyses and Examples

This section of the *SAR Activity Review* outlines examples and patterns of suspicious activity reported in a SAR. Financial institutions may find this information a valuable tool in alerting themselves to trends and patterns of suspicious activity discovered elsewhere.

Securities & Futures Industries SARs: The First Quarter

Brokers or dealers in securities, one segment of the securities and futures industries, were required to report suspicious financial activity using FinCEN Form 101, also known as Suspicious Activity Reports by the Securities and Futures Industries (SAR-SFs), beginning in January 2003.[15] By mid-March, a total of 119 entities had filed 555 SAR SFs. Statistical analysis of SAR-SF data revealed several interesting trends and patterns, which are provided below.

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 SARs can specify more than one type of suspicious activity per form.)

[15] The final SAR filing requirements are pending for Futures Commission Merchants & Introducing Brokers in Commodities. However, those industries may voluntarily file SARs by submitting a SAR-SF.

TYPES of SUSPICIOUS ACTIVITY REPORTED	SARs	Percentage of Total SARs 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 from $0 to as high as $5 billion.[16] Twelve SAR-SFs reported amounts of at least $100 million, including five filed in New York, three in San Francisco, three in Iowa, and one in Miami.

The table below provides a synopsis of the volume of SAR-SFs filed by amounts.

[16] The SAR with the largest suspicious amount was filed in January 2003 by a securities firm located in the Midwest. An employee at a client bank referred a man to the securities firm who inquired about investing as much as $100 million in government securities. The man then called a regional representative of the securities firm and left a message requesting that the securities representative call him concerning an investment of as much as $5 billion. The man told the firm's representative that he worked for a religious organization that did missionary work in South American and African countries. He claimed his organization had received some large gifts from wealthy families and wanted to purchase large amounts of short-term securities, backed by some type of arrangement with a bank in the Far East. He said his group would not deposit funds with the firm; rather, he wanted the firm to write trade tickets with the bank in the Far East, which were covered by some type of letter of credit or similar arrangement. The securities firm told the man that they "couldn't do business that way," and the discussion ended. The firm subsequently filed a SAR due to the man 's suspicious comments.

SUSPICIOUS AMOUNTS REPORTED	SARs	Percentage of Total SARs Reviewed
Blank (no amount reported) or $0	83	15.0%
$1 – $9,999	90	16.2%
$10,000 – $99,999	228	41.1%
$100,000 – $999,999	78	14.1%
$1,000,000 – $9,999,999	38	6.8%
$10,000,000 – $99,999,999	26	4.7%
$100,000,000 and over	12	2.2%

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.]

TYPES of FINANCIAL INSTRUMENTS REPORTED	SARs	Percentage of Total SARs 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 SAR-SFs 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).

Fifty-nine SAR-SF filers checked the "Market where traded" box (item 23S on the form), but only 15 actually listed a market. Five filers listed "over-the counter," while three listed the N.Y. Stock Exchange; two listed ASE (American Stock Exchange); two listed NASD (National Association of Securities Dealers); two listed CINN (Cincinnati Stock Exchange); and one listed NBB (Over the Counter Non-Bulletin Board). One SAR specified "precious metals" under commodity type.

Information Reported by Financial Institutions

Six banks and 113 other entities, including at least three foreign bank subsidiaries, in 30 states and Puerto Rico, filed SAR-SFs. Other branches of these filers were found in 11 additional states and the District of Columbia (D.C.)—resulting in suspicious activity being noted in 41 states, D.C. and Puerto Rico. The States of New York, Washington, and California had the highest volume of reporting institutions for both categories.

STATES of FILING INSTITUTIONS	SARs
Alabama	4
Arkansas	1
Arizona	1
California	45
Colorado	8
Connecticut	5
Delaware	2
Florida	10
Georgia	2
Iowa	6
Illinois	3
Kentucky	1
Massachusetts	9
Maryland	6
Maine	1
Michigan	29
Minnesota	12
Missouri	15
North Carolina	14
Nebraska	20
New Jersey	43
New York	228
Ohio	1
Pennsylvania	14
South Carolina	1
Tennessee	1
Texas	5
Vermont	1
Washington	57
Wisconsin	9
Puerto Rico	2

OTHER REPORTING BRANCHES	SARs
Alabama	5
Arkansas	2
Arizona	8
California	60
Colorado	15
Connecticut	7
District of Columbia	3
Delaware	2
Florida	33
Georgia	19
Hawaii	4
Iowa	5
Illinois	12
Indiana	3
Kentucky	2
Louisiana	1
Massachusetts	10
Maryland	11
Maine	1
Michigan	8
Minnesota	7
Missouri	12
North Carolina	14
Nebraska	17
New Hampshire	2
New Jersey	24
New Mexico	1
Nevada	6
New York	131
Ohio	3
Oklahoma	1
Oregon	1
Pennsylvania	20
Rhode Island	1
South Carolina	1
Tennessee	7
Texas	22
Utah	1
Virginia	4
Washington	60
Wisconsin	6
West Virginia	1
Puerto Rico	2

Subject Information

Most SAR-SFs (320 or 57.7%) did not specify an occupation for the subject. The occupations listed on the SAR-SFs are grouped into categories in the table below. (Note: Since some SARs have multiple subjects, the total will exceed 555.)

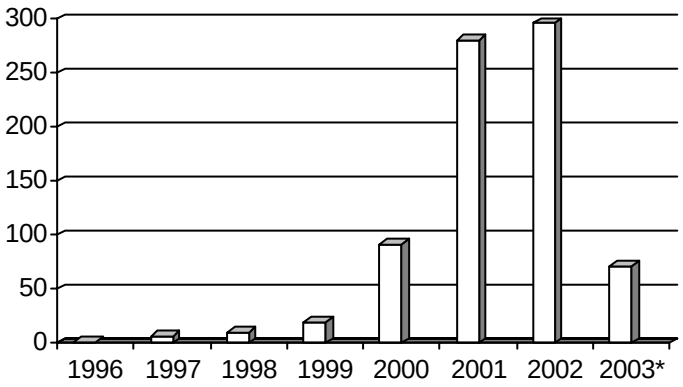
OCCUPATION	SARs	Percentage of Total SARs Reviewed
Unknown / Unemployed / None Listed	320	57.7%
Business	59	10.6%
Professional	35	6.3%
Investment	32	5.8%
Administrator	22	4.0%
Retired	16	2.9%
Mortgage / Finance / Pawn	15	2.7%
Self-Employed	13	2.3%
Property	13	2.3%
Homemaker	13	2.3%
Service Workers	12	2.2%
Banking	10	1.8%
Health	9	1.6%
Administrative / Clerical / Customer Service	7	1.3%
Information Technology	5	0.9%
Student	4	0.7%
Art / Music / Athletics	3	0.5%
Farming / Ranching	2	0.4%
Non-Profit	1	0.2%

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 discussed online or Internet banking increased considerably. One reason for the increase

may be the addition of "Computer Intrusion" as a specific violation type, which was incorporated into the depository institution SAR Form (TD F 90-22.47) in June 2000.



* Through 3/18/03

Statistical Overview

A total of 291 separate financial institutions, including six foreign banks licensed to conduct business in the United States, filed the above-mentioned 776 SARs. The SARs were filed in 47 states,[17] the District of Columbia and Puerto Rico. The five states with the most filings were: California (145 or 18.7%), Texas (80 or 10.3%), New York (55 or 7.1%), Florida (52 or 6.7%), and Ohio (30 or 3.9%). Those five states filed 362 or 46.6% of the SARs in this study.

The 776 SARs identified 983 violations.[18] The most frequently cited violations were:

1. Other – 198 SARs or 20.1%
2. Check Fraud – 190 SARs or 19.3%
3. Computer Intrusion – 160 SARs or 16.3%
4. BSA/Structuring/Money Laundering – 145 SARs or 14.8%
5. Counterfeit Check – 78 SARs or 7.9%

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

---

[17] SARs were not filed in Mississippi, Rhode Island and Wyoming.
[18] SARs may cite no violation, one violation or multiple violations.

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, 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. Before the rapid rise and fall of the dot-coms, there were approximately 60 Internet banks.

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 Service Providers (ISP)

Internet Service Providers (ISPs) for banks offer their clients valuable services. ISPs can maintain a close watch on the websites they provide to banks, detecting intruders who are trying to deface, tamper with, or hack into their operating systems. In this study, 122 separate bank branches in 31 states filed 126 SARs as a result of information received from their ISPs. The banks responsible for filing those SARs appeared to be small to mid-sized community or county banks.

Trends and Patterns

The mostly commonly reported violations consisted of many different scenarios. The following is a synopsis of that reported activity.

Violation Category	Number of SARs	Percentage of SARs Reviewed
Check Fraud and Counterfeit Checks	112	14.4%
BSA/Structuring/Money Laundering	100	12.8%
Identity Theft	80	10.3%
Computer Intrusion or Hacking	46	5.9%
Wire Transfer Fraud	35	4.5%
Defalcation/Embezzlement and Misuse of Position or elf-dealing	32	4.2%
Forgeries	25	3.2%
Check Kiting	19	2.4%
Schemes or Scams	12	1.5%

The vast majority (90%) of SARs reporting check fraud or counterfeit checks involved accounts opened through a bank's Internet website using identities of real persons. Small opening deposits, usually around $100 and consisting of cash, money orders or third-party checks, were conducted in person or mailed to the bank. Shortly thereafter, worthless or counterfeit checks were deposited into the accounts. Some characteristics of those checks included alteration to the payee line; checks chemically washed or otherwise altered; and computer generated counterfeit checks. Before the fraudulent items were detected and returned, ATM/debit card withdrawals, point-of-sale transactions, or the transfer of funds via the Internet to another account at a different bank, depleted the deposited funds.

One bank headquartered on the West Coast filed 68% of the 100 BSA/Structuring/Money Laundering SARs. Almost all of those SARs reported structuring of cash deposits and withdrawals. The remaining 32% 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. Additionally, five SARs filers reported customers attempting to open accounts for the sole purpose of obtaining online banking capabilities.

SARs citing identity theft reported the use of individuals' personal information (i.e., social security numbers, personal identification numbers) to access and steal funds in existing bank accounts through on-line transactions, change mailing addresses, order checks on-line, open new depository accounts, or obtain fraudulent loans or credit and debit cards through financial institutions' Internet websites. Frequently, reported activity involved suspects who gained access to victims' accounts to establish online bill payment services. Once activated, the

suspects were able to authorize payments from the victims' accounts to the suspects' creditors.

Financial institutions reported computer intrusion or hacking attempts perpetrated randomly upon accounts or institution websites, possibly to access customer accounts or information. Often, suspects made numerous attempts within a short time period to penetrate the institutions' firewalls. One SAR reported that 126 accounts were compromised during such an intrusion. On two occasions, hackers defaced bank websites with obscenities or anti-American sentiments.

Real Estate Industry – Sales & Management

This information is presented to provide financial institutions with trends and patterns of suspicious activity relating to sales and management in the real estate industry.[19] In an effort to identify areas of potential concern, two preliminary analytical studies were performed in the last 18 months. The results of these studies will further a continuing dialogue with, and study of, the industry's potential money laundering vulnerabilities.

During the fall 2002, FinCEN completed a study of the trends and patterns observed in SAR filings related to the real estate industry, specifically related to the sale and/or management of real estate. The review period for that study encompassed the period of January 2001 to August 2002. Recently, an update to the study covering the period of September 2002 to March 2003 was completed to identify any significant changes in reporting of suspicious activity since the original was conducted. The following provides a comparative analysis of the two studies.

The number of records retrieved for the period January 1, 2001 through March 31, 2003 demonstrated a steady increase in the number of SARs filed on persons or businesses identified as having occupations involving the sale and/or management

[19] In April 2003, FinCEN issued an Advance Notice of Proposed Rulemaking to solicit public comments on a wide range of questions pertaining to the requirements of Section 352 of the USA PATRIOT Act that financial institutions establish anti-money laundering programs, as the BSA defines a "financial institution" to include "persons involved in real estate closings and settlements." The solicitation of public comments included how to define "persons involved in real estate closings and settlements," the money laundering risks posed by such persons, and whether any such persons should be exempted from any requirement that might be imposed.

of real estate. Financial institutions filed 43% more such SARs in 2002 than were filed in 2001.

In the first study, a search of the SAR data retrieved a total of 1,554 unique SAR records for the period January 1, 2001 to August 31, 2002. (In the twelve-month period for 2001, 850 SARs were filed; during the eight months in 2002 from January through August, 704 SARs were submitted.) A steady increase was noted in the number of filings beginning with the third quarter of 2001. This increase indicated an increasing pattern of identification of suspicious activities by persons listed as having real estate related occupations. This trend continued in the fourth quarter 2002 through the end of the first quarter 2003. During this latter period, a total of 1,224 unique SAR records were identified.

Statistical Information (September 1, 2002 to March 31, 2003)

The following chart relates the types of violations, total numbers and percentages of SARs reported by financial institutions:

Violation Type	Number of SARs	Percentage of Total SARs Reviewed
A – BSA/Structuring/Money Laundering	888	67.0%
S – Other	105	7.9%
P – Mortgage Loan Fraud	99	7.5%
C – Check Fraud	58	4.4%
D – Check Kiting	54	4.1%
N – False Statement	36	2.7%
E – Commercial Loan Fraud	27	2.0%
H – Counterfeit Check	13	1.0%

Violation amounts ranged from $0 to $150 million.[20] Seventy-two SARs reported amounts of $1 million or more.

[20]An MSB in a large metropolitan area in the Midwest filed the $150 million SAR. No narrative was included in the SAR; thus, the suspicious activity that prompted this SAR is unknown.

During the research period, 374 financial institutions in 44 states,[21] Puerto Rico and the Virgin Islands filed SARs related to real estate sales or management. Nineteen of the 374 institutions were foreign corporations licensed to conduct business in the United States. Approximately 60% of the SARs were filed in four states: California (32%); New York (14%); Texas (7%) and Florida (7%). These findings were consistent with the pattern of geographic filings in the initial study.

The following table identifies the types of institutions and volume of SARs submitted.

Type of Financial Institution	Total Number of SARs Filed
Full Service Banks[22]	328
Credit Unions	14
Investment and securities companies	13
Financial advisors	4
Money services businesses	4
Mortgage banks	4
Holding companies	3
Travel agencies	1
Insurance companies	1
Credit card banks	1
Internet banks	1
Total Financial Institutions	374

Highlighted Violations Types

The narratives of a random sample of 580 SARs (approximately 47% of the total retrieved SARs) were reviewed for this updated study. The Financial Action Task Force (FATF) recently included real estate in the list of operations that require financial oversight. That, coupled with a recent trend to reduce restrictions on foreign investments, and a corresponding increase in foreign investments in real estate, focused attention on reports that described funds either coming into or going out of the United States.

---

[21]No financial institutions from the states of Maine, North Dakota, South Dakota, Rhode Island, Vermont, Wyoming or the District of Columbia filed SARs for the search criteria specified in this study.

[22]Full service banks are defined as banks offering a full range of financial services, i.e., checking accounts, savings accounts, and commercial and private loans.

Terrorism

One SAR narrative described activities that were suspected of being terrorist-related. A bank filed a report on a customer who gave his occupation as real estate investor. The customer received funds from an airline company previously sanctioned by OFAC for conducting a transaction with a Specially Designated National (SDN). The customer, in turn, wired funds to South America and to another domestic bank. Additional research concerning the details of the domestic wire transfer revealed an additional SAR regarding the receiver of the funds. In this second SAR, the suspect—the same individual that received the funds described in the first SAR—was receiving suspicious transfers from the Middle East and Canada.

Cash Structuring

Transaction structuring was described in 329 (57% of the sample) of the 580 sampled SARs; seven described foreign fund transfers. The reports in this category described customers suspected of structuring transactions to avoid having a CTR filed. Thirty-two of the sampled SARs noted that the customer changed the transaction when informed of the CTR requirement. Eleven of the sampled narratives described structuring in wire transfers. The transactions were specifically described as "cash" in 184 (56%) of the sampled SARs in this category. All other reports identified the transactions as "checks," "wire transfers," "money orders," or "traveler's checks."

BSA/Structuring/Money Laundering

The narrative described activity as "suspicious" in 111 (19%) of the 580 sampled reports. The narratives did not describe "Money Laundering" or "Structuring," but stated that the filer believed some type of illegal activity could be involved. SARs specifically describing structuring and money laundering were broken out of this category for a more in-depth study, which will appear later in this section. The filers reported eight of the suspicious activities directly to law enforcement.

Fraud

Fraud was cited in 68 (12%) of the SARs sampled. Types of fraudulent activity were: Loan Fraud (54), Identity Fraud (6), Flipping (4),[23] Advanced Fee Fraud (2), and Securities Fraud (2).

---

[23]Flipping is the buying and selling of the same property within a short period of time with the intention of making a quick profit. This activity is often coupled with loan and other forms of fraud.

There was no mention of money transferred into or out of the country for this category. The reporting financial institutions contacted law enforcement agencies directly about 12 (2%) of those incidents.

Check Fraud/Check Kiting

Check Fraud was cited in 34 (6%) SARs; Check Kiting was cited in 25 (4%) SARs of the 580 narratives sampled. Reporting institutions notified law enforcement of about 12 (20%) of the suspicious incidents.

Money Laundering

Money Laundering was cited in 12 (2%) sampled SAR narratives. Filers reported one of those incidents directly to law enforcement. Two of the reports involved foreign money transfers.

Summary

The trends and patterns revealed in the initial report continued in the update period. The same four states identified in the initial report as having the majority of the suspicious activity (California, New York, Florida, and Texas) were identified in the update period as the locations having the most activity. The same types of financial institutions filed the reports for both periods.

The most common classification type was BSA/Structuring/Money Laundering. Filers classified 445 (76%) of the sampled SARs as this type of suspicious activity. Transaction structuring, the most frequently described activity, appeared in 329 (or 57%) of the 580 sampled reports. Structuring transactions to avoid BSA reporting and recordkeeping requirements is prohibited under 31 U.S.C. 5324 and is often an indication of further illegal activity.

The narratives described the suspicious transaction as "cash" in 219 (or 38%) of the total sampled reports. With the exception of real estate rentals (which comprised only 6% of the occupations in the sampled reports), real estate is not largely considered to be a cash industry. Large cash payments in a non-cash business could be an indication of money laundering activity.

Thirty-six SARs (or 6% of the sampled reports) described funds either entering or leaving the United States. Following is the geographic breakdown of the locations from which money was transferred into or out of the United States.[24]

[24]Three SARs described accounts with money transfers both into and out of the United States.

FOREIGN MONEY TRANSFERS	INCOMING	OUTGOING
Africa	1	0
Caribbean	1	3
Europe	4	4
East Asia	2	3
Middle East	2	2
North America	1	1
South America	4	5
Southeastern Asia	1	5
Total	16	23

Section 3 - Law Enforcement Cases

This section of *The SAR Activity Review* provides law enforcement agencies with the opportunity to summarize investigative activity in which SARs and other BSA information played an important role in a successful investigation and/or prosecution of criminal activity. Each issue of *The SAR Activity Review* includes new examples based on information received from law enforcement. Other law enforcement cases will be posted shortly on the FinCEN website, www.fincen.gov in the Regulatory/SAR Information section of the website. In this issue of *The SAR Activity Review,* we are featuring a special update on the results of FinCEN's new system implemented under Section 314(a) of the USA PATRIOT Act.

USA PATRIOT Act Section 314(a) System

Under Section 314(a) of the USA PATRIOT Act, FinCEN issued a rule which established a system to enable law enforcement officials, who were investigating terrorist financing cases as well as major money laundering cases, to relay targets of investigation to thousands of financial institutions for real time responses. Following a brief moratorium from November 2002 to January 2003, which suspended all Section 314(a) activity, the System resumed operation in February 2003. From February through October 20, 2003, FinCEN submitted 167 Section 314(a) requests to financial institutions on behalf of 11 individual Federal law enforcement agencies. The agencies only submitted 314(a) requests in the conduct of the following significant criminal investigations—Terrorism (60) and Money Laundering (107).

The 167 cases submitted included 962 subjects of interest. Through October 20, 2003, 6,397 positive responses were received from financial institutions, which were forwarded to the law enforcement requesters by FinCEN. A total of 2,136 related to terrorism cases and 4,261 related to money laundering cases. Of the 6,987 total responses received from financial institutions, 338 were inconclusive.

Law enforcement requesters were asked to provide information about the utilization of the financial information received from the first quarter 314(a) requests. About 60% of the requesters responded with the following results as of September 2003:

- 586 new accounts located;

- 24 new transactions identified;
- 216 Grand Jury Subpoenas served;
- 11 Search Warrants executed;
- 6 National Security Letters issued;
- 16 Administrative Subpoenas/Summons issued; and
- 2 individuals arrested.

Law Enforcement Feedback

Following the moratorium, the feedback from law enforcement 314(a) requesters has been overwhelmingly positive. An ICE[25] Officer wrote, "314(a) information provided by the FI was pivotal to the investigation." An IRS Special Agent said, "314(a) information helped the case tremendously. Accounts not previously known were identified and points of contact at the bank were established." Another IRS Agent said, "314(a) process is great and valuable. The information request identified domestic account activity previously unknown." The agent said he would definitely use the process again. An FBI agent said, "I think the system is fantastic. In all my government years, I really haven't seen a system work this efficiently. I was able to identify over 40 accounts for my subject. I don't think I would have been able to identify some of these accounts without this mechanism."

Investigations Assisted by SARs

Numerous SARs and CTRs Aid in Hawala Investigation

In March 2002, the FBI opened an investigation into the activities of a hawala dealer in the western United States. Limited initial information received from a citizen complaint prompted a query of the BSA database. The query yielded 30 SARs and 13 CTRs, which were instrumental in identifying numerous bank accounts used by the hawala. Over a five-year period, the subjects, all Iraqi immigrants, wired in excess of $4 million from a U.S. bank to accounts in Amman, Jordan. From there, most of the money was illegally smuggled into Iraq in violation of the Iraqi Sanctions Act. Other funds were sent to Syria, Saudi

[25] Bureau of Immigration and Customs Enforcement

Arabia, Iran, UAE, Chile, Ukraine, and Denmark. Over 535 customers were identified in multiple states from California to New York. Subjects were depositing cash and checks into their U.S. bank accounts issued from banks and individuals located in several midwestern and western states. Prior to the implementation of the USA PATRIOT Act in 2001, one subject independently wired over $1.8 million to a subject in Jordan.

The main operator of the hawala was indicted in October 2002 on one count of Title 18 USC §1960. Three search warrants were executed that same month on the main subject's residences. In addition, four bank account seizure warrants were served covering seven bank accounts, resulting in over $19,000 in seized funds. In January 2003, this subject pled guilty to operating an illegal money transmitting business. He was sentenced in March to four months in prison and a $10,000 fine. Charges against additional subjects are anticipated. *(Source: FBI)*

SAR Leads to Conviction of Iraqi Money Launderer

In September 2003, an Iraqi national was sentenced in federal court after pleading guilty in June 2003 to one count of 18 USC 1956 (h): conspiracy to launder money with the underlying offense of 18 USC 1957 (engaging in monetary transactions in property derived from a Specified Unlawful Activity [SUA]) in connection with a prior arrest in December 2002.

This investigation was initiated when a Corporate Security officer at a major domestic financial institution advised an ICE[26] office that the defendant was transferring funds to Iraq via Jordan and the United Arab Emirates (UAE) in violation of the Iraqi Sanctions Act, IEEPA, etc. SARs were filed prior to, and after receiving this information.

The investigation revealed that in 1996, the main target of this investigation initiated his money laundering operations in conjunction with his brother-in-law in Baghdad, to facilitate the worldwide purchase of various commodities. In 1998, the subject began operating as a money transfer business, which utilized over 30 domestic agents throughout the United States and collected in excess of $28 million over a 20-month period from Iraqi nationals and other individuals of Middle Eastern descent. Analysis of records recovered from various warrants showed that $12 million went directly into Iraq. The target utilized these funds to

[26]In March 2003, the U.S. Customs Service, among other agencies, moved into the new Department of Homeland Security and became part of the Bureau of Immigration and Customs Enforcement (ICE). Some cases appearing in Section 3 were investigated and adjudicated prior to this transition while this agency was known as the U. S. Customs Service (Customs).

purchase commodities from businesses worldwide that were then illegally transshipped through various trading companies in the UAE and Jordan into Iraq in violation of international sanctions. *(Source: ICE)*

SAR Reports Structuring by Unlicensed MSB

ICE agents and analysts in a state in the Southwest developed information from a SAR that an out-of-state business was structuring deposits of large sums of cash and was operating as an unlicensed MSB. During a two-month period, this business made outgoing wire transfers totaling approximately $1.2 million to Pakistan, India, and Bangladesh. As a result, a state seizure warrant was executed on the bank accounts of this business and agents seized $346,700.58. The business eventually forfeited approximately 75% of the seized proceeds to the state. *(Source: ICE)*

SAR Identifies Suspects Involved in a Nigerian Advance Fee Scam

Two suspects, a husband and wife, had been corresponding with individuals in Nigeria for several months concerning a transfer of $30 million from Nigeria to their bank account. The suspects, skeptical of the promises made by the foreign philanthropist, performed their own investigation via the Internet. They visited the USSS website which discusses Advance Fee Scams and warns the public not to get involved with solicitors of such schemes.

The couple confronted their Nigerian solicitor about what they had learned. The solicitor assured them that no risk was involved. In fact, he had an investor that would "loan" the couple the "advance fees" that normally accompany the transaction. At that time, the couple was willing to continue with this scam as long as they would not suffer financially. The solicitor forwarded an altered check for $185,000 to the couple who deposited the check into their bank account. They immediately wired the majority of the funds to the solicitor, while keeping $10,000 for themselves. During a post arrest interview, the couple, both whom had criminal histories of fraud, admitted that they were very suspicious during this incident but were not worried since they did not risk any of their own money. They kept the $10,000 in case this was a scam so they would at least get something for their troubles. The check was eventually returned as an altered item and the bank of deposit took a financial loss. While depositing the check into their bank account, which had an average monthly balance of $400, the couple lied to the bank teller, stating that the check was proceeds of a family inheritance. The bank filed a SAR related to their $10,000 loss. During a subsequent search of the

couple's residence, agents with the USSS seized 20 guns (illegally possessed by the convicted felons) and $10,000 in cash. The suspects were arrested, tried, and convicted of violations of the state's Penal Code for burglary and grand theft and received three years in prison. *(Source: USSS)*

SARs Result in Sentencing of Family Members in Bankruptcy Fraud Case

Three family members pled guilty to charges including bankruptcy fraud, structuring, providing false statements, and mail fraud for their involvement in a bankruptcy fraud scheme that included structuring transactions and concealing funds from credit card companies and financial institutions, funds which the main target had obtained as credit card advances and home equity loans. During a bankruptcy proceeding, the primary subject concealed the fact that the funds had not been spent, but had been placed in various accounts under the targets' control. The investigation was initiated from the filing of numerous SARs by a financial institution over an extended time period, which drew notice of the IRS. The SARs stated that the subjects were making numerous currency deposits in amounts of $9,900 at multiple locations of the financial institution on the same day. Based on the information developed from the SARs, search and seizure warrants were obtained during the course of the investigation.

Criminal information filed with the court to support the guilty pleas relayed that the subject filed a petition under Chapter 7 of Title 11, in which the subject claimed an indebtedness of approximately $390,000 owed to credit card companies and financial institutions. However, as mentioned previously, the primary subject concealed the fact that the funds had not been spent but rather were placed in various accounts under the targets' control. After the primary subject was discharged from bankruptcy, she structured funds from various bank and brokerage accounts for the purpose of bringing back to her ownership, funds which she had previously placed elsewhere in the names of others as a way of avoiding her creditors in her personal bankruptcy. During the conduct of this activity, the target structured approximately $184,300 in an attempt to avoid CTR filings.

Analysis of bank records subpoenaed during the course of the investigation revealed that the primary subject had rented a safe deposit box, which was controlled by all three defendants. On the application, she listed the other two defendants as co-renters for that box. The safe deposit box's access records indicated that the primary subject had accessed her safe deposit box on numerous occasions on the same day, or within days of making cash withdrawals from one of her bank accounts.

According to court records filed, as the primary target was involved in the structuring of deposits, the other subjects applied for and were granted federal financial aid to attend medical school. The two subjects listed minimal or no cash of their own on their financial aid applications. In addition, the applications claimed that their parents had minimal cash in their accounts and had no earned income. However, bank records revealed that brokerage accounts controlled by all three defendants, including one parent, carried balances exceeding $200,000. These individuals received approximately $29,800 of federal money in student loans.

At the time of their guilty plea, the court ordered the defendants to forfeit the following assets: a 1997 Mercedes Benz E420; three bank accounts containing approximately $145,133; a safe deposit box containing $174,000 in cash; and two brokerage accounts valued at approximately $31,800. Subsequently, the primary subject was sentenced to serve 15 months in prison, followed by 36 months of probation. The other two defendants were sentenced to 36 months probation. In addition, these individuals had their respective educational grants withdrawn (due to the false loan applications) and must pay restitution on the amounts received. As a result of their felony convictions, the two were dropped from their respective medical programs.

Agencies participating in this investigation include the IRS-Criminal Investigation, FBI and The Department of Education Inspector General. *(Source: IRS-Criminal Investigation)*

SARs Assist in Bankruptcy Bust-Out Scheme Investigation

SARs helped identify additional aliases, associates, and businesses of an individual that acted as a credit card 'bust-out' recruiter. As a recruiter, the subject assisted other individuals (usually from the same ethnic group and experiencing financial or personal difficulties) in escaping their fiscal problems. The subject convinced his recruits that he had contacts with credit card companies, that these contacts had the ability to work through their financial problems, and that there was an opportunity to earn extra cash in the process. To accomplish this, the subject usually had a recruit provide many of his/her personal identifiers to him, including social security number and date of birth. Sometimes, the recruit was directed to provide any of his existing credit cards to the subject. Subsequently, the subject and recruit reached an agreement, usually splitting the proceeds from the recruit's credit card charges in some manner. The charges were typically for merchandise, cash advances, and airline tickets. The subject assisted the recruit in applying for more credit cards, many times using false personal information to obtain these cards.

All credit cards were issued in the recruit's name, although the subject made most of the charges. In order to increase their credit limits, the recruit paid off the credit cards with bad checks, resulting in immediate credit being extended for the accounts. Then, the recruit used the same credit cards, charging up to their limits for a second time. By the time the bad checks were returned, the recruit usually had charged double the limit for each credit card.

This activity continued for two to three billing cycles before the credit card companies froze the accounts and began the collection process. When the recruit's debts piled up, the subject advised the recruit to file for bankruptcy and any outstanding debts to creditors were then discharged.

To date, the subject is believed responsible for over $6 million in bankruptcy filings by his recruits although the subject apparently never personally filed for bankruptcy. The investigation continues into the bank fraud (mainly check kiting) committed by the subject. SAR data has been useful in documenting the volume of fraud committed solely by the subject. The total amount is believed to be in the millions of dollars, with a substantial portion of the proceeds possibly wired out of the country. *(Source: FBI)*

SARs Connect Multiple Subjects to Large Scale Investment Scam

In April 2002, predicated by numerous SAR filings by two large banks, the FBI initiated an investigation into an investment scam. The SARs were filed on numerous personal and business accounts with no obvious relationships to one another. Bank personnel eventually linked all accounts through the identification of common depositors and/or individuals making withdrawals. For example, in a single month, one account received between $200,000 and $600,000 in wire deposits, money orders, and checks. The funds were then withdrawn daily in cash or used to send wire transfers. Additional funds were used for purchases of money orders and money grams, and to send other Fed wires. Over a two-year period, between $10-20 million moved through the account. The source of the funds was allegedly from a fraudulent insurance bond investment scheme involving dozens of subjects. Many of the victims were financially ruined, losing their homes and businesses.

In early 2003, 22 search warrants were executed in three states. To date, eight criminal complaints and eight indictments have been filed resulting in seven arrests and one notice to appear. In addition, this case has generated asset seizures of $2.4 million in currency and bank accounts thus far. Additional arrests, indictments and seizures are anticipated. *(Source: FBI)*

SAR Suspect Convicted of Forging U.S. Treasury Checks

A bank filed a SAR reporting the deposit of U.S. Treasury checks to an account held by a deceased customer (a retired government employee) receiving monthly retirement benefits. The bank determined that its customer died in 1998. For two and one half years following the customer's death, her daughter forged her deceased mother's signature on the U.S. Treasury checks, deposited the funds into the account, and lived off the proceeds which totaled approximately $100,000. As a result of the SAR, the USSS initiated an investigation, which resulted in the arrest and subsequent conviction of the suspect for violation of 18 USC 510, Forging U.S. Treasury Checks. She received five years of federal probation and was ordered to pay restitution to the U.S. Treasury Department. *(Source: USSS)*

SARs Identify Money Laundering of Proceeds from the Sale of Marijuana

Four individuals involved in the distribution and sale of marijuana were sentenced to prison terms ranging 12 to 21 months followed by up to 36 months probation. These sentences resulted from guilty pleas by the targets on one count each of money laundering for the manner in which they handled between $350,000 and $600,000 in funds traceable to marijuana trafficking. According to court papers filed, two of the defendants structured cash derived from the sale of marijuana into various accounts and then transferred the funds by check, wire transfer, or cash to the other two targets, operators of a concert promotion and nightclub business. These individuals subsequently used this business as a way to launder the money from the marijuana distribution business, disguising the money as legitimate business receipts and mixing it with proceeds from promotions and concerts.

This investigation was initiated from the analysis of two SARs filed by two separate financial institutions, regarding the deposits of cash to the target's bank accounts. Many of the deposits were for amounts under $10,000 and structured to avoid the currency reporting requirements. The structured transactions were conducted by depositing cash on consecutive days, making several deposits on the same day, and spreading the deposits among bank accounts at different institutions.

Agencies participating in this investigation include the IRS-Criminal Investigation, the FBI and a local police department. *(Source: IRS-Criminal Investigation)*

State and Local Law Enforcement Use of SAR Data

The following cases obtained through the FinCEN Gateway Program[27] illustrate state and local governments' use of SAR data.

State & Federal Agencies Seize $8.9 Million—Brought Together By Gateway Alert Match Program

The Pennsylvania (Pa.) Office of Attorney General's Asset Forfeiture and Money Laundering Section conducted pro-active targeting research on SARs that initiated a Pa. State Grand Jury Money Laundering investigation on two suspects.

FinCEN's Gateway Program was utilized by the Pa. Attorney General's Office, Bureau of Narcotics Investigation to conduct research in the Currency and Banking Retrieval System (CBRS) for additional BSA reports related to the two suspects. Those reports included 147 CTRs, 11 Currency Transaction Reports by Casinos (CTRCs), six Report of Foreign Bank and Financial Accounts (FBARs), four Report of International Transportation of Currency or Monetary Instruments (CMIRs), and seven SARs. The investigator stated they had the suspicious activity, but had no specified unlawful activity.

Subsequently, as a result of the Gateway Alert Program, a case match with the Immigration and Naturalization Service (INS), Philadelphia Office, was found. These two investigations eventually became one with federal prosecution. The PA Attorney General's Office performed the money laundering investigation, and the INS performed the specified unlawful activity investigation, which was Harboring, Transporting, Encouraging Illegal Aliens to Reside in the United States. This activity was in violation of Title 8, USC, Section 1324 and 1324(a). The subjects were also charged under Title 8, USC, Section 1324 a, Unlawful Employment of Aliens, and Title 18 USC, Section 1961 (1), Racketeering Activity, sub-section (F) any act which is indictable under the Immigration and Nationality Act, Section 274 (relating to bringing in and harboring certain aliens.)

---

[27]The Gateway Program enables federal, state, and local law enforcement agencies to have direct, on-line access to records filed under the BSA.

The first phase of the investigation culminated on April 10, 2002 with the execution of ten search warrants in five states, and court orders freezing 36 bank accounts, and lis pendens placed on two pieces of real estate. The liquid assets amounted to $3.9 million, and the real estate amounted to $4.8 million. The total amount of assets seized is $8.7 million to date. This case is presently ongoing. *(Source: Pennsylvania Attorney General's Office)*

BSA Filings Identify Financial Scams Bilking Investors out of $2.2 Million

In May 2003, two individuals pled guilty to first-degree money laundering charges. One defendant was sentenced to 12 years incarceration, and ordered to pay $500,000 to the Anti-Money Laundering Profiteering Fund. The second defendant was sentenced to 18 years incarceration. A month earlier, in a separate jurisdiction, a third defendant pled guilty to money laundering charges and was sentenced two years supervised probation.

Others involved in this scam of bilking investors were charged in a second financial scheme exceeding $1.6 million. The primary suspect and a second individual are awaiting sentencing on conspiracy, which occurred between May 1999 and July 2000. During that time, the primary suspect allegedly assumed a false identity to cash forged checks from a major futures trading association, payable to the fictitious person and totaling more than $1.6 million. Also, the same suspect allegedly cashed investors' checks totaling more than $150,000, payable to the suspect's business. The checks were negotiated at a check cashing service with offices in two counties.

The two men allegedly told investors that their money would be invested in the primary suspect's business, purported as an e-commerce and information service company. The men also allegedly tried to cash a forged check at a check cashing service. The check was issued from a car dealership, payable to the suspect's business, for $50,000.

The New Jersey Division of Criminal Justice (NJDCJ) conducted a review of the CBRS database, the repository for BSA reports, relating to all subjects and their businesses. The review was accomplished through the use of FinCEN's Gateway Program. Forty-nine CTRs, two CTR-Cs, one FBAR, and two SARs were located. The subsequent investigation was initiated after the pro-active search and discovery of records in CBRS. The search identified the subjects and the check cashing services they used. Copies of the cashed checks, payable to various west coast-based medical labs, were obtained from the check cashers. Those checks amounted to approximately $10 million. Those checks were associated with the

first scam initiated by the subjects through their business. The FBAR identified one of the business' bank accounts in the Far East. The two SARs were useful, since one described numerous structured deposits, and the other identified the person who cashed 14 stolen checks. *(Source: New Jersey Division of Criminal Justice)*

Section 4 - Tips on SAR Form Preparation & Filing

How to Improve the Quality of SAR Reporting

Overall, financial institutions continue to do an excellent job of reporting suspicious activity, but improvements can be made. As reported in Issue 5 of *The SAR Activity Review - Trends, Tips and Issues*, law enforcement and regulatory agencies (the primary users of SAR data) continue to report to FinCEN that SARs are filed with missing and incomplete data. Less than 2/100ths of one percent of SARs filed since 1996 had no suspect identification, no activity characterized, and no sufficient narrative to explain what activity was being reported. This situation most often occurs when filers check the activity characterization box marked "Other" but fail to specify the suspicious activity on the line provided. The problem is compounded when filers enter the phrase "see attached" in the "Narrative" section of the form and attach items such as spreadsheets or computer printouts as documentation. When SAR forms are received at the IRS Detroit Computing Center (DCC), only information in an explicit, narrative format is keypunched; thus, tables and other numeric data contained in spreadsheets are not included in the narrative. SARs that do not specify the suspicious activity being reported or fail to provide an explanation as to what led the institution to become suspicious are of minimal value to law enforcement or regulators. Please do not include any supporting documentation with your filed report; keep the information in your records for five years. Law enforcement will contact you at the appropriate time to review the information.

The value of the "Narrative" section of the report to law enforcement cannot be stressed enough. The care with which it is written may make the difference in whether or not the described conduct and possible criminal nature are clearly understood by law enforcement and regulators. Financial institutions must review and follow the instructions found in the "Suspicious Activity Information Explanation/Description" section of the SAR form. In addition, always select and mark the appropriate box(es) in the "summary characterization of suspicious activity" section.

During the year from July 1, 2002 to June 30, 2003, financial institutions (as defined by 31 CFR 103) filed approximately 300,000 SARs. The following issues were identified:

- Four percent were filed without a suspect name.
- Eight percent did not list an address for the suspect.
- Twenty-three percent did not provide the suspect's social security number.
- Four percent did not provide any indication of what suspicious activity occurred.
- Six percent did not complete the narrative.

There are valid reasons why some of this data could be missing. FinCEN requests that you review your SAR reporting program and make enhancements if required. If the data (name, address, or SSN) is not available or is unknown, please indicate "not available" or "unknown" in the data box requesting the information. This is an excellent opportunity for your back office reviewers to improve your SAR reporting program.

FinCEN, in consultation with the federal regulators, is producing a guidance package consisting of three parts: a report entitled, "Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative" and two power point presentations, "The Suspicious Activity Report Form" and "Keys to Writing a Complete and Sufficient SAR Narrative." This package will be available shortly on the FinCEN website, www.fincen.gov.

How to Complete the SAR Form

At the top of any SAR form is the statement, "Always complete entire report." On some SAR forms,[28] this is appended with a statement that items denoted by an asterisk (*) are considered critical.

[28]SAR-MSB (Form TD F 90-22.56), SAR-SF (FinCEN Form 101), and SAR-C (FinCEN Form 102).

What constitutes "completing" a SAR?

A SAR form has been completed when all of the available information has been entered and responses such as "none" or "not available" have been entered in any blank critical field. These responses are words, phrases, or codes that inform FinCEN that data for that item is unavailable or not applicable, and has not been simply overlooked by the filer. Items are considered critical when they contain important information required for law enforcement investigations, such as: subject name; subject identifying number and address; type of suspicious activity; and a detailed narrative.

These responses are needed for several reasons. First, they tell law enforcement and data collectors that the filer considered the item. Second, such responses indicate the requested information was not available at the time of filing, did not exist, or did not apply to the suspicious activity. Third, such responses assist in the processing of BSA data by eliminating the need to correspond with the filers to obtain what appears to be missing information.

Responses commonly used in SARs to clarify what appears to be missing data, their definitions, and examples of how they are used:

Term	Explanation
None	The requested information does not exist.
Not Applicable	The requested information is not relevant to the subject or suspicious activity.
Unknown	The filer does not know the requested information.
XX	This applies only to two digit fields such as state or country. The filer does not know a two-digit code indicating the country or foreign state/territory of the subject. This is the same code already in use by institutions that are approved for Magnetic Media filing.

General Tips for Using These Types of Responses in SARs

1. If the SAR instructions require a specific response for an item, use that response. For example, a list of country codes may show "XX" as the abbreviation used for a country that is unknown to the filer. This is the case for the Casino SAR form. Therefore, filers that do not know which country the suspicious activity is related to should put "XX" in the country code item.

2. Do not further abbreviate responses such as "unknown" as it could cause further confusion. For example, "unknown" abbreviated as "UK" may mislead law enforcement into thinking the suspicious activity is related to the United Kingdom.

3. Critically important fields of information such as: subject name; subject identifying number and address; type of suspicious activity; and the narrative, etc., should have "unavailable" in the field if no information is indeed available. Doing so will eliminate the need for the processing center to contact the filer asking for what might appear to be an oversight.

4. SARs are only as valuable as the data reported on them. Reports that do not identify a suspect, do not identify one of the "Types of Suspicious Activity" and do not provide a narrative are of little use to law enforcement. Therefore, filers are reminded to pay particular attention to these fields and to supply as much information as possible regarding the identity of the listed suspect(s).

It's worth restating; SARs are only as valuable as the data reported on them. Fields of information left blank are of no use to law enforcement and may actually cause more confusion. If certain data is unavailable, does not exist, or is not applicable, law enforcement wants to know it. Please tell us this by using one of the terms defined above. Using one of the above terms will clear up any ambiguity.

How to Report Potential Terrorist-Related Activity

General Instructions for Completing the SAR Form

All of the SAR forms now permit the filer to report terrorist financing by checking a box in the suspicious activity section of the SAR. Filers should then complete the most important section of the SAR, the Narrative, by describing the suspicious transaction as completely as possible, including the following information, if applicable: any correspondent bank name/account information; names/locations of business entities; names of cities, countries and foreign financial institutions linked to the transaction, especially if funds transfer activity is involved; and account numbers and beneficiary names.

Specific Instructions for a Particular Industry

- Depository institutions reporting potential terrorist-related activity on Form TD F 90-22.47 are requested to check the "Terrorist financing" box in Part III, item 35(t) of the form. However, in some situations, the suspicious activity may also involve money laundering or some other suspicious activity. Therefore, the institution should also check the additional appropriate box(es) in item 35.

- Casinos and card clubs reporting potential terrorist-related activity on FinCEN Form 102 (SAR-C) are requested to check item 26(p) in Part II. If the suspicious activity also involves money laundering, or some other suspicious activity, the appropriate line in item 26 should also be checked.

- MSBs reporting potential terrorist-related activity on Form TD F 90-22.56 should check Box 28(c) (Terrorist financing) on Part II, Line 28. If the suspicious activity also involves money laundering or structuring, Box 28(a) and/or (b) should also be checked.

- Securities and futures industry entities reporting potential terrorist-related activity on FinCEN Form 101 (SAR-SF) are requested to check item 30(q) in Part II. If the suspicious activity also involves money laundering, or some other suspicious activity, the appropriate additional line in item 30 should also be checked.

Regardless of which form is used, all filers should ensure that the Narrative includes as much detail as possible regarding the potential terrorist-related or other suspicious activities. Remember: do not include supporting documentation with the SAR. The supporting information must be maintained for five years with the filer's copy of the filed SAR.

Please also remember that a SAR should not be filed because of a person's ethnicity, nor should it be filed solely because a person appears to have the same name as individuals identified by the media as terrorists.

Transactions to, from, or conducted by persons with possible affiliations with jurisdictions associated with terrorist activity should not be the only factor that prompts the filing of a SAR. However, this information should prompt additional scrutiny of such transactions and then should be considered in conjunction with other relevant information in deciding whether a SAR is warranted, as set forth in 31 CFR 103.18 and the regulations prescribed by the bank regulatory agencies, such as a lack of any apparent legal or business purpose to a transaction or series of transactions. Resources that should be consulted about such jurisdictions include: the State Department's list of State sponsors of terrorism; the Treasury Department's OFAC's lists of foreign terrorists; and FATF's list of non-cooperative countries and territories (NCCTs).

Tips from the Regulators

The following guidance is provided by the federal regulatory authorities and/or FinCEN.

Importance of having a Centralized Review of SARs

Financial institutions might consider establishing a centralized location for the review and processing of SARs. Nevertheless, as part of an institution's internal controls, it is especially important that adequate management review of the SAR contents and filing is completed before the SAR is submitted. If a centralized review process is employed, financial institutions should ensure that the identity of the bank, its primary regulator, and the location of the transaction are clearly indicated on the SAR and that the SAR is not filed under the name and location of the centralized processing unit.

Also, when appropriate, the financial institution may wish to seek legal counsel during the filing process.

New Depository Institution SAR Form

FinCEN, in conjunction with the regulatory agencies, has amended the Depository Institution SAR form (Form TD F 90-22.47) in order to include two new boxes, one for terrorism and one for identity theft. Financial institutions are encouraged to start using the new SAR form as soon as possible. The new form became available for use on July 1, 2003. While use of the new form is not mandatory until January 1, 2004, immediate use of the form is encouraged in order to give law enforcement more information about crimes involving terrorism and identity theft.

With regard to instances of possible terrorism, identity theft and computer intrusions, it is recognized that the dollar thresholds for filing may not always be met. Financial institutions are encouraged to file, nonetheless, in appropriate situations involving these matters, based on the potential harm that such crimes can produce. In addition, financial institutions are reminded that even when the dollar thresholds of the regulations are not met, the institutions have the discretion to file a SAR. In such situations, the financial institutions will still enjoy the safe harbor provided for in the statute.

With regard to identity theft, financial institutions should keep in mind that the victim's name should not go on the first page of the SAR under the field "suspect." If there is no identifiable suspect, that field should state "unknown." The victim's name should be stated in the "Narrative" section of the form.

Filling out the SAR Form

If the SAR is filled out at a centralized location within the financial institution or at the holding company level, it is extremely important that the SAR identify the actual financial institution involved, the location of the office or branch where the activity took place, and the correct primary federal regulator. (In situations where the holding company or an affiliate is filing the SAR, the primary federal regulator of the financial institution involved may not be the regulator of the holding company or the affiliate.)

With regard to the designation of the type of violation that is involved, financial institutions are strongly encouraged to use the "Other" box only when absolutely necessary, that is, when it is clear that none of the other available boxes is applicable. Overuse of the "Other" box distorts the data in the system and makes it more difficult to search for particular types of violations. A recent review of the SAR database indicated that there were many instances in which the "Other" box

was checked when there were more applicable, specific boxes that should have been checked.

Closing of an Account

There is no requirement in the SAR regulations that a financial institution must close an account that is the subject of the filing of a SAR. The decision to maintain or close an account is left to the financial institution. However, if an account is involved in a suspicious or potentially illegal transaction, the institution should examine the status and history of the account thoroughly and should determine whether or not the institution is comfortable with leaving the account open. It is often advisable to include legal counsel in making this decision. If the institution is aware that the reported activity is under investigation, it is strongly recommended that the financial institution notify law enforcement before closing an account.

Filing a Corrected SAR Form

If the financial institution determines that it has made an error in completing a SAR, it should refile the SAR in its entirety with the corrected information, making sure to mark the box entitled "Corrects Prior Report." The institution should then describe the changes to the form in the Narrative section. If the institution wants to file a SAR providing updated information or showing related transactions, it should file a new SAR and, in the Narrative section of the SAR, explain that the SAR represents updated or related information in connection with a previously filed SAR.

Reporting a Loss

It is important that financial institutions, when filing SARs, report not just the amount they may have lost, but also the amount involved in the transaction or activity. Similarly, financial institutions should consider thresholds for reporting not just on the amount lost, but also on the amount involved in the transaction or activity.

Contacting Law Enforcement

Financial institutions are reminded that in situations involving violations requiring immediate attention, such as when a reportable violation (e.g., money laundering scheme, terrorist financing, or other financial crime) is ongoing, the financial institution shall immediately notify, by telephone, appropriate law enforcement and financial institution supervisory authorities. Also, remember that direct contact by telephone or in person with law enforcement and supervisory authorities to report possible suspicious activity does not relieve the institution from filing a timely SAR to the IRS DCC.

Where to Send The Completed SAR Form

Depository Institution SARs (Treasury Form TD F 90-22.47) filed in paper format should be mailed to:

Detroit Computing Center
P.O. Box 33980
Detroit, MI 48232-0980

SARs for Money Services Businesses (Treasury Form TD F 90-22.56) filed in paper format should be mailed to:

Detroit Computing Center
ATTN: SAR-MSB
P.O. Box 33117
Detroit, MI 48232-5980

SARs for the Securities and Futures Industries (FinCEN Form 101) filed in paper format should be mailed to:

Detroit Computing Center
Attn: SAR-SF
P.O. Box 33980
Detroit, MI 48232-0980

SARs for Casinos and Card Clubs (FinCEN Form 102) filed in paper format should be mailed to:

Detroit Computing Center
ATTN: SAR-C
P.O. Box 32621
Detroit, MI 48232-5980

Depository Institution SARs, SAR-MSBs, SAR-SFs or SAR-Cs filed by magnetic media/diskette format, should be mailed to:

IRS Detroit Computing Center
Attn: Tape Library
985 Michigan Ave.
Detroit, MI 48232

Section 5 - Issues & Guidance

This section of the *SAR Activity Review* discusses current issues raised with regard to the preparation and filing of SARs. This section is intended to identify SAR-related issues and then provide meaningful guidance to filers; in addition, it reflects the collective positions of the government agencies that require organizations to file SARs.

Frequently Asked Questions (FAQs)

FinCEN's Regulatory Helpline[29] is available to financial institutions to provide guidance on various topics related to the BSA. In order to better assist with compliance questions, information is offered in this section concerning some of the most common FAQs posed to the Helpline relating to two current "hot" topics, Section 314(a) issues and suspicious reporting for MSBs.

Section 314(a) of the USA PATRIOT Act

How do I change my point of contact for 314(a)?

Although FinCEN and the federal regulators are modernizing the process to update, change, add, or delete your financial institution's point-of-contact (POC) information on FinCEN's distribution list for receiving Section 314(a) Information Requests, currently you are required to contact your primary federal supervisory agency to make those changes. Financial institutions subject to supervision by one of the five Federal "banking" regulators should also provide information for Section 314(a) POCs on the institution's quarterly Call or Thrift Financial Report.

The following items must be provided to update or add your financial institution's POC information: financial institution name and charter number or other identifier; POC name and title, mailing (street number, P.O. Box, city, state and zip code) and e-mail addresses; and telephone and facsimile numbers.

[29] The telephone number for FinCEN's Regulatory Helpline is 1-800-949-2732.

Please find your institution's primary federal supervisory agency in the below list and forward the above information to them.

Board of Governors of the Federal Reserve System

Contact information:

e-mail: patriotact@frb.gov
fax: (202) 736-5641

Commodity Futures Trading Commission

Contact information:

e-mail: AMLstaff@cftc.gov
fax: (202) 418-5528
Questions: Helene D. Schroeder, Special Counsel, Division of Clearing and Intermediary Oversight
(202) 418-5424

Federal Deposit Insurance Corporation

Contact information:

All changes must be made through the quarterly call report.
(800) 688-FDIC
e-mail: Insurance-Research@FDIC.gov

Office of the Comptroller of the Currency

Contact information:

e-mail: nationalbankinfo@occ.treas.gov
fax: (202) 874-5301

Office of Thrift Supervision

Contact information:

e-mail: usap.contact@ots.treas.gov
fax: (202) 906-6326

National Credit Union Administration

Contact information:

Please contact your designated NCUA examiner or state supervisory authority

National Association of Securities Dealers (NASD)

Contact information:

e-mail: antimoneylaundering@nasdr.com
Questions: Emily Gordy, Kyra Armstrong
(202) 728-8221

New York Stock Exchange (NYSE)
Contact Information:
e-mail: SKasprzak@NYSE.com
fax: (212) 656-2068
telephone: Stephen Kasprzak (212) 656-3000

How can I get a copy of the search instructions and FAQs for 314(a)?

Financial institutions that need a copy of the FAQs and instructions can request these documents by calling FinCEN's Regulatory Helpline at (800) 949-2732 or by e-mail at sys314a@fincen.treas.gov. FinCEN will only send the instructions and FAQs to a financial institution's designated POC that was provided to FinCEN by the financial institution's regulator.

How can an institution tell if a 314(a) match is a true "hit" that requires a positive response to FinCEN and not a false positive?

If an institution is unsure if a 314(a) match is a true hit, FinCEN suggests that the institution call the agent associated with the case. The case agent's contact information is listed at the top of each information request.

Reporting Suspicious Activity by MSBs

Which MSBs are required to report suspicious activities?

The requirement that MSBs file a SAR applies only to money transmitters, currency dealers or exchangers, and issuers, sellers or redeemers of money orders and traveler's checks. It does not apply to check cashers or to issuers, sellers, or redeemers of stored value. However, any MSB may voluntarily file a SAR for any suspicious transaction that it believes is relevant to the possible violation of any law or regulation, but whose reporting is not required. A statutory safe harbor from liability for reporting applies whether the filing is voluntary or required.

When must MSBs begin to report suspicious activities to FinCEN and how are they to be reported?

Money transmitters and issuers, sellers, or redeemers of money orders and traveler's checks were required to begin reporting suspicious transactions occurring after December 31, 2001. Currency dealers or exchangers were required to file SARs beginning on August 11, 2003. MSBs must use the

SAR form especially designed for them, the SAR-MSB, TD F 90-22.56. This SAR-MSB form should be sent to the: Detroit Computing Center, ATTN: SAR-MSB, P.O. Box 33117, Detroit, MI 48232-5980.

When is an MSB required to file a SAR?

An MSB is required to file a SAR on a transaction or series of transactions conducted or attempted by, at, or through the MSB if both of the following occur:

- The transaction or series of transactions involves or aggregates funds or other assets of $2,000 or more, AND
- The MSB knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part) falls into one or more of the following categories:

    1. involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation; or
    2. is designed to evade any BSA regulations; or
    3. has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the MSB knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
    4. involves use of the money services business to facilitate criminal activity.

An issuer of money orders or traveler's checks is required to report a transaction or pattern of transactions that involves or aggregates funds or other assets of $5,000 or more when the identification of the transactions as suspicious is derived from a review of clearance records or other similar records of money orders or traveler's checks that have been sold or processed.

An MSB is required to file each SAR no later than 30 calendar days after the date of the initial detection by the MSB of facts that may constitute a basis for filing a SAR.

I'm worried about being sued by the customer if I file a SAR. What protection do I have?

Federal law (31 U.S.C. 5318(g)(3)) provides a "safe harbor" or protection from civil liability to financial institutions and their directors, officers, employees or agents that report suspicious activity to FinCEN or appropriate law enforcement or supervisory agencies. A financial institution is prohibited from notifying any person involved in the transaction that the transaction was reported on a SAR (31 USC 5318(g)(2)). If you receive a subpoena for a SAR, or a request of any kind to produce a copy of a SAR (other than a request by FinCEN, or an appropriate law enforcement or supervisory agency), you should contact FinCEN's Office of Chief Counsel at 703-905-3590 immediately; federally regulated depository institutions should also contact their regulator.

I'm worried about damaging someone's reputation or getting someone in trouble if I'm wrong about a transaction being suspicious. What happens to SARs after they are filed and who looks at them?

A SAR is not an accusation against someone or an allegation that they have committed a crime. A SAR indicates that a transaction may be suspicious. SARs are not disseminated to the public; rather, they are provided only to appropriate law enforcement and financial supervisory agencies.

Is an MSB required to have an Anti-Money Laundering (AML) Compliance Program? If so, what is an AML Program?

All MSBs are required by law to have an effective anti-money laundering (AML) compliance program. The regulation requiring MSBs to develop and maintain an AML compliance program as of July 24, 2002, or 90-days after establishment, is contained in 31 CFR 103.125.

Each AML program must be commensurate with the risks posed by the location, size, nature and volume of the financial services provided by the MSB. For example, a large money transmitter with a high volume of business located in the Los Angeles area is at higher risk than a small check casher with a low volume of business located in Boise. Therefore, the large California money transmitter would be expected to have a more complex AML compliance program, commensurate with its higher risk, than the smaller Idaho check casher, who is at lower risk of being used to facilitate money laundering. An effective AML program is one designed to prevent the MSB from being used to facilitate money laundering.

An AML compliance program must be in writing and must:

- incorporate policies, procedures and internal controls reasonably designed to assure compliance with the BSA;
- designate a compliance officer responsible for day-to-day compliance with the BSA and the compliance program;
- provide education and/or training of appropriate personnel; and
- provide for independent review to monitor and maintain an adequate program.

Filing SARs on OFAC List or 314(a) Matches

A verified match with an entity on an OFAC list that involves funds in an amount above the applicable SAR filing threshold should trigger a SAR filing requirement. Any transaction with, by or for a person listed by OFAC is unlawful. Therefore, when a financial institution verifies that it has a match with the OFAC list, it always will have identified at least a potential violation of law. It is important, however, to verify "hits" identified by a financial institution's OFAC filters to ensure that there is a true match, looking not only at the full name, but the address and any other identifiers that have been provided by OFAC, to avoid false positives for common names, which, we are informed, has been most prevalent in the Kingpin sanctions program. If a financial institution has any questions about its OFAC obligations and responsibilities, it should call the OFAC Hotline at (800) 540-6322.

In contrast, a match with a named subject issued pursuant to the Section 314(a) process does not automatically require the filing of a SAR. Section 314(a) requests seek to identify assets associated with a particular suspect. There may be nothing about the particular account or transaction found in response to a Section 314(a) request that is inherently illegal. A financial institution should review the account activity or transaction(s) relating to the named subject for suspicious activity, and, if appropriate, file a SAR predicated upon the totality of the circumstances and the account activity, in addition to reporting the Section 314(a) match to FinCEN.

BSA Guidance – The IRS Detroit Computing Center (DCC), the FinCEN Helpline, & the FinCEN Website

The IRS DCC may be contacted at 1-800-800-2877 to assist you with questions regarding the use of the revised CTR exemption regulations (31 CFR Section 103.22(d)(2)), completion of the Designation of Exempt Person form (TD F 90-22.53), completion of the CTR form (Form 4789), as well as CTR paper or magnetic filing issues. For other BSA-related questions, you may call FinCEN's Regulatory Helpline at 1-800-949-2732, leave a detailed message, including your question, your name, the name of your financial institution, and your telephone number. Someone from FinCEN's Office of Regulatory Programs will return your call promptly. Finally, the answers to a number of FAQs are found on the FinCEN website at www.fincen.gov/reg_faqs.

Florida Appeal Court Reverses Lower Court Order to Produce SAR

On July 23, 2003, a state appeal court in Florida issued an opinion reversing a lower court order that required a bank to produce a SAR to another bank that was a defendant in civil litigation. International Bank of Miami v. Shinitsky, 2003 Fla. App. Lexis 11090. The case is notable because the state appeal court recognized the importance of SAR confidentiality by granting a remedy that is only available when a very high standard is met – a showing that the petitioning bank would suffer irreparable harm and that the lower court had departed from the essential requirements of law. The case also illustrates the harm that can result when banks fail to notify their regulator and FinCEN that a demand has been made for a SAR.

The proceeding arose from a case brought against various defendants for an alleged investment fraud scheme, including the bank at which the major fraud perpetrator had its account. The plaintiff sought documents from another bank that had maintained an account for the alleged perpetrator, including any SARs filed on it. Over the bank's objection, the trial court ordered the production,

subject to a confidentiality order. The objecting bank did not notify FinCEN or its regulator (the OCC) of the proceeding. Over 18 months later, a bank defendant who had not had access to the SAR under the confidentiality order, moved for production of the SAR to it. That motion, too, was granted over the producing bank's objection. At that point, the bank notified FinCEN and the OCC. FinCEN's Chief Counsel provided a declaration in support of the bank's motion to reconsider the order, which was denied. (The OCC also denied the defendant bank's request to it for production of the SAR.) The bank then sought immediate relief from the court of appeal through a procedure known as a petition for certiorari.

The Florida court of appeal granted the petition. Although the SAR had already been produced, it had been subject to a confidentiality order, so the court found that the cat was "half-in and half-out of the bag." The situation could therefore be remedied, and the court determined that the risk to bank employees from SAR production and the effect on customers constituted irreparable harm. On the merits, the court of appeal found the trial court was clearly wrong in ordering the SAR to be produced, finding, in line with the federal courts to address the issue, that the SAR was subject to an unqualified privilege. The order, therefore, was reversed. Although the appellate court found that the initial order to produce the SAR had been obeyed and not appealed, and therefore could not be challenged, it tried to undo some of the harm from the prior production of the SAR to the plaintiff, warning the trial court that if the plaintiff tried to modify the confidentiality order in order to use the SAR in court proceedings, the trial court should approach any such request with caution.

Financial institutions should always notify their regulator and FinCEN when they receive any document request, subpoena, or other demand for a SAR, other than those authorized by the applicable SAR rule.

Section 6 – SAR News Update

PACS Is Being Expanded

As reported in Issue 5 of *The SAR Activity Review*, FinCEN has significantly eased the cost of filing BSA forms by instituting the Patriot Act Communication System (PACS). PACS is a highly secure method of filing BSA forms through the Internet, including single forms and batches of forms, using the filing institutions existing anti-money laundering systems and processes, and an Internet connection. It enhances the security of the BSA form filing process through the use of digital signatures and secure Internet connectivity. The system accelerates the delivery of BSA information to federal and state law enforcement and it reduces the expense to the financial institution by eliminating the need for magnetic tapes and paper forms. An institution incurs no cost to sign up or use PACS.

When PACS was first released on October 1, 2002, the system was capable of processing forms filed primarily by depository institutions—the CTR and the SAR forms. The system's first year of operation proved quite successful, with approximately 650,000 BSA forms processed. The system has already saved both the government and the industry scarce human and capital resources, and, most importantly, has reduced the amount of time required to get these critically important reports to law enforcement.

Building on the system's success, FinCEN is currently expanding the capability of PACS to allow for the filing of the following BSA forms:

- Suspicious Activity Reports by the Securities and Futures Industries FinCEN Form 101
- Suspicious Activity Reports by Money Services Business — TD F 90-22.56
- Suspicious Activity Reports by Casinos and Card Clubs — FinCEN 102
- Currency Transaction Report by Casinos — FinCEN Form 103 (formerly Form 8362)

FinCEN has been testing this new capability since August 2003 with members of the MSB and the Securities and Futures industries; since the beginning of September 2003, testing has been underway with members of the casino industry. This "pilot test" will ensure that the technical approach is sound and is useful to the

industry. PACS became available to all filers of FinCEN Form 101, TD F 90-22.56, FinCEN Form 102 and FinCEN 103 on October 1, 2003.

For further information about PACS, visit the PACS website, www.pacs.treas.gov.

Non-Cooperative Countries and Territories (NCCTs)

FinCEN conducted SAR research on the existing nine FATF designated NCCTs[30] (as of June 2003) encompassing statistical data and ensuing trends from SARs filed on the NCCTs through December 2002. With the exception of Nauru and Guatemala, SAR filings increased for NCCTs after FATF designation. A common thread among these countries and the activities reported was suspicious and/or fraudulent wire transfer activity. With the exception of Nigeria, wire transfer activities accounted for the most prevalent description in the narratives for the "BSA/Structuring/Money Laundering" violation and in the "Other" violation category. A variety of scenarios accompanied this activity, including structured deposits followed by wire transfers; wire transfers followed by withdrawals in a foreign location via ATM or check; and use of a correspondent banking relationship with a U. S. bank, which was unable to verify a physical presence for the foreign bank. A number of other schemes were reported in the narratives, including Nigerian 419 scams; large cash payments ($9,900 to $20,000) on small or zero balance credit card accounts followed by "Credit Balance Refund Checks" sent to account holders within days of the cash deposits; attempts to open accounts with invalid or altered identification documents; fraudulent letters of credit offered as security on loans in an alleged precious metals scam and in attempts to purchase securities. Possible direct or indirect connections with Internet gambling activities were reported, plus a scheme that involved the purchase of merchandise with counterfeit checks in amounts greater than the agreed upon purchase price, followed by wire transfer of the excess funds back to the customer before discovery of the counterfeit check(s).

[30] The current list of NCCTs designated by the FATF are: Cook Islands, Egypt, Guatemala, Indonesia, Myanmar, Naura, Nigeria, Phillipines and Ukraine.

Financial Industries Required to File SARs

The following table identifies financial institutions with current or proposed SAR filing requirements.

Type of Financial Institution	SAR Required?	Type of SAR Form	Effective Date	Filing Amount	Regulation
Depository Institutions: Banks Bank Holding Companies Non-bank Subsidiaries of Bank Holding Companies Savings Associations Saving Association Service Corporations Edge and Agreement Corporations U.S. Branches and Agencies of Foreign Banks Credit Unions	Yes for all	TD F 90-22.47 SAR	April 1996 (revised form effective July 2003)	$5,000 or more in funds or other assets	31 CFR 103.18
Money Services Businesses: Money Transmitters Issuers, Sellers, or Redeemers of Money Orders Issuers, Sellers, or Redeemers of Traveler's Checks U.S. Postal Service Currency Dealers or Exchangers	Yes for all	TD F 90-22.56 SAR-MSB	January 2002 January 2002 January 2002 January 2002 August 2003	$2,000 or more in funds or other assets; $5,000 or more for issuers of money orders & traveler's checks identifying transactions through the clearance process	31 CFR 103.20
Casinos and Card Clubs	Yes	FinCEN Form 102 SAR-C	March 2003	$5,000 or more in funds or other assets	31 CFR 103.21
Securities and Futures Industries: Securities Broker/Dealers ("BD") Futures Commission Merchants ("FCM") Introducing Brokers in Commodities ("IB")	 Yes Proposed Proposed	FinCEN Form 101 SAR-SF	 January 2003 Proposed Proposed	$5,000 or more in funds or other assets	31 CFR 103.19 Pending Pending
Insurance Companies Issuing, underwriting or reinsuring a life insurance policy Issuing, granting, purchasing or disposing an annuity contract Issuing, underwriting or reinsuring any insurance policy with investment features similar to a life insurance policy or annuity contract, or which can be used to store value and transfer value to another person	 Proposed Proposed Proposed	SAR-IC	 Proposed Proposed Proposed	$5,000 or more in funds or other assets	 Pending Pending Pending
Mutual Funds Open-end Investment Company registered or required to register with the SEC	Proposed	FinCEN Form 101 SAR-SF	Proposed	$5,000 or more in funds or other assets	Pending

Section 7 - Industry Forum

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into some aspect of compliance management or fraud prevention that presents their view of how they implement the BSA within their institution. Although the Industry Forum Section provides an opportunity for the industry to share its views, the information provided in it may not represent the official position of the regulators.

Some Tips for Auditing the Suspicious Activity Reporting Program

By Alan S. Abel representing The American Institute of Certified Public Accountants to the Bank Secrecy Act Advisory Group[31]

The Bank Secrecy Act (BSA) requires independent testing of the compliance program to determine whether the program is suitably designed and operating effectively. Because suspicious activity reporting (for purposes of this article, small sar) is an important component of Anti-Money Laundering (AML) and BSA programs increasingly across financial services and now even other sectors, the accounting profession plays an ever-larger role in fulfilling this requirement.

The auditor's primary objectives in independently reviewing a SAR program include:

- Identifying material program weaknesses, control deficiencies and opportunities for program, process, and control enhancement and reporting them to senior management and the board
- Assisting senior management with identifying money laundering and other financial crime vulnerability in the context of risk focused supervision, in four key regulator defined risk areas: compliance, reputational, strategic, and operational. The flip side of this is helping senior management better assess and manage risk.

[31] Alan Abel also is Global Leader, Anti-Money Laundering Compliance and Risk Management Services for PricewaterhouseCoopers LLP.

- Performing work that may be useful to regulators in conducting their supervisory examinations.[32]

In addition, it is not unconventional for the auditor to identify unusual and suspicious activity in connection with performing the SAR program audit procedures.

Here then are some criteria and leading practices that auditors may wish to consider in developing and administering an audit program to review and independently test a SAR program.

The Internal Environment

Before drilling down into sar processes and controls surrounding those processes, the auditor should consider the "big picture" – the overall internal control environment of the enterprise as it relates to sar. This means getting a sense of the "tone-at-the-top" of the organization, i.e. what is senior management's and the boards' attitude, posture and message about integrity, ethical values, and competence? Are the right messages sent internally and externally about the importance of complying with the letter and spirit of the law and about protecting the enterprise, its people, assets, operations and reputation from money launderers, money laundering, and related financial crime? Does the Board-approved policy framework (and, by the way, are the policies Board-approved?) contain a clear policy and commitment to identify and report suspicious activity? When talking to employees, does one get a sense that these values are effectively communicated and shared? Do employees across the enterprise have a positive attitude, understand what unusual and suspicious activity are and the importance of identification and reporting to management? Do they know what to do and who to contact? How frequently does this subject show up on internal communications?

Written Compliance Program

The auditor should look for evidence of compliance program documentation about unusual and suspicious activity identification and reporting at three levels:

- Level I: Board-approved policy framework (see above). The auditor needs to gain an understanding of the specific BSA SAR regulatory requirements

[32]Note: Supervisors are generally neutral as to whether AML /BSA programs should be performed by internal or external auditors. What they *do* care about is the quality of the work, i.e. that the work is performed by seasoned professionals with appropriate technical AML / BSA expertise.

that apply to the enterprise. Is the organization currently required to comply with BSA SAR enterprise-wide? Is there a voluntary SAR policy anticipating future requirements or because senior management and the board believe that they are doing the right thing regardless of requirements? Does the policy fully comply with regulatory requirements? Are aspects of the policy more stringent than required? (A SAR policy that exceeds the enterprise' regulatory requirements is perfectly acceptable – it reflects a more conservative risk appetite which few would question. It is important, however, to understand what it is). The auditor should also review the agendas and minutes of senior management and board meetings to determine whether the right discussions and actions are taking place to support a well-considered SAR policy and to get a sense of future plans or intentions to review or modify the policy.

- Level II: Enterprise-wide standards and guidance. The auditor should determine what enterprise-wide standards and guidance are articulated and promulgated by senior management that support a SAR program. What high-level standards and guidance has senior management developed and communicated to employees about the nature of unusual and suspicious activity and how to seek it out and recognize it when encountered? Does management communicate to employees the conduct and response that is expected of them? Is internal and external guidance (e.g. the SAR Activity Review) well communicated and accessible? How well does senior management articulate and convey the importance of Know Your Customer (KYC) principles and provide guidelines on how to apply them to the organization? Does senior management encourage employees to seek out and stay abreast of external guidance? How frequently do employees actually do this?

- Level III: Implementing, operating policies and procedures. Many business organizations confuse policies with procedures, as is frequently evident from reviewing compliance program documentation, and accounting professionals frequently assist their clients with revising their written compliance programs accordingly. Here's the distinction in a nutshell — policies are the "what" and procedures are the "how." Successful implementing and operating policies and procedures will robustly apply the Board-approved policy framework and the enterprise-wide standards and guidance to each of the business units and support areas of consequence. In other words, each of these areas should have a set of tailored policies and procedures that clearly describe how the overall SAR policy, standards and guidance for the enterprise as a whole applies to

them – the types of unusual and suspicious activity likely to be encountered, roles and responsibilities, specific operating procedures and controls? Are the required actions and follow-up clearly articulated? What information should be produced and what are the appropriate channels of communication? The Sar is, of course, time-sensitive and this message should come through loud and clear in the procedures.

Robust Risk Assessment Process

In the realm of suspicious activity, one size does not fit all. Merely taking SAR forms and instructions and broadcasting them across the enterprise will not likely be very effective for getting results. As is the case for other key elements of an AML and BSA compliance program, the suit needs to be tailored – i.e. the sar process needs to be risk and business based. Business units need to assess what types of unusual and suspicious activity are more likely to occur and what employees are more likely to encounter in their respective areas. To get a good sense of whether the enterprise has a sound risk assessment process in place, auditors should look to see whether there is a hands-on AML / BSA committee, usually chaired or coordinated by the AML / BSA compliance officer) made up of individuals who properly represent the business units and support areas of consequence. Among their committee obligations and assignments, members should be actively engaged in periodic risk assessment and reporting results to the committee. The output of risk assessment should be a blueprint for the types of unusual and suspicious activity that the employees of respective areas are more likely to encounter. Frequently and a leading practice, Management will prepare a risk assessment survey (designed with SAR or other reportable conditions in mind) that will be administered by the committee. In particular, this exercise should be valuable for engaging employees in the risk assessment process, with the obvious, hoped-for benefits. Therefore, a robust risk assessment exercise is an important way of determining whether a SAR program is suitably designed and operating effectively.

Also, it is a leading practice for an enterprise-wide SAR program to be active (as opposed to passive) and pre-emptive. The more effective SAR program is one characterized by high-energy outreach versus one where management passively waits for internal reports to (maybe) come forward. Getting to and sustaining the state of “high-energy active” requires continuously deploying the other program elements and identifying and engaging opportunities for continuous improvement.

Risk Profiling and Benchmarking

As part of the risk assessment process, it is a good idea to periodically compare and report to senior management the enterprise' sar performance with industry performance. (Of course, the leading source of sar performance benchmarking information is the SAR Activity Review). The auditor may wish to make an independent determination and compare it to management's. It is important for compliance management to highlight, report and explain material SAR filing variances to senior management. There are usually some very compelling reasons for variances – everyone has a different risk profile, and no two enterprises have the same profile of customers, products and services, geographies, distribution channels, employees, and other business relationships. However, it's a good idea for senior management to articulate the enterprise' risk profile in any event and to explain SAR filing performance variances in the context of that profile. Supervisors and law enforcement may walk in the door with a set of expectations with respect to character and volume of SARs, and senior management should be prepared to present, discuss and explain their SAR filing performance.

Training and Awareness

Training is of course, a core BSA program requirement. The auditor should determine whether or not there is a sufficient KYC and SAR component to the training materials. The auditor should assess the effectiveness of training through talking to employees and through reviewing test results where applicable. Training materials should show signs of freshness and meaningfulness.

Centralized Reporting

While not a hard and fast requirement, it is a good practice for SARs to emanate from one portal out-the-door to law enforcement. Ideally, the enterprise will have an internal mechanism for employees to report events or situations that they believe are unusual or suspicious that is separate and distinct from the SAR that may ultimately be prepared and filed. (Most enterprises have a name for this internal mechanism or report that distinguishes it from "SAR" to avoid confusion). There should be controls in place to make sure that only specifically authorized and designated individuals are part of the event escalation, analysis and reporting stream. Your supervisors and law enforcement expect to see SAR filings come from one or very few designated individuals — usually an AML / BSA compliance officer. The auditor should test SARs filed to determine whether these procedures are being followed and should note exceptions.

Auditors should ask for process flow charts or descriptions of reporting process flows, and the test the process to see if it works as designed.

For frequently compelling and also "legacy" reasons, enterprises frequently have their sar processes fragmented, (the euphemisms are "shared, distributed, and allocated") and often in a manner where corporate security (internal law enforcement) handles the "fraud SARs" and compliance handles the money laundering, structuring, and BSA-related SARs (or a distinction is made between the "internal" SARs and the "external" SARs). While this approach may be functional in many respects, sar process fragmentation allows opportunities for control deficiencies. SARs and their supporting cases may "fall through the cracks," and "need-to-know," while important to the objective of confidentiality, frequently becomes a barrier to the balanced level of communication required for an effective sar process.

It is the better practice for one office (usually the AML /BSA Officer) to be the conductor of the SAR orchestra of players. Obviously, corporate security plays a critical role in conducting and supporting investigations. In fact, auditors should review corporate security and other investigations, analysis, and reporting staff in view of caseload to determine whether there are sufficient, competent, technical resources to adequately cover the volume of existing and anticipated activity.

Sound Judgment and Quality Process

As indicated above, it is important to distinguish the internal detection and escalation process from the external SAR filing process. Employees should be sufficiently trained and engaged, and written policies and procedures should be sufficiently clear and robust so that the internal detection, reporting and escalation process can be effective. Typically, employees prepare an internal report of unusual or suspicious activity in consultation with a supervisor and the designated compliance liaison. The internal report should be quickly escalated for analysis and investigation (i.e. the internal report becomes a case) that is tracked, and then quickly routed or further escalated to a committee to review the case and to make the "suspicious" determination. The committee members (the decision-makers) should be persons of sufficient authority and judgment to make the determination. It is conventional for the AML / BSA Officer to present the case and make a recommendation to the Committee. Because SAR filings are time sensitive, it is a good practice for a draft SAR, already reviewed for completeness, quality, and risk to be presented to the Committee for case review. The auditor should obtain a thorough understanding of the entire sar process and the controls in place governing the process.

Quality Case Tracking

Regulators typically require businesses to maintain a "SAR log." While minimally adequate to "check off the box," anything less than a flexible, storable, well-maintained case-tracking database does not generally provide adequate control over the SAR process, except for a lower-risk, lower-reportable event volume environment. Frequently, a conventional software spreadsheet or low-end data base management system with indexing and sorting capability will suffice.

While not all internally reported incidents, events or situations will ultimately result in a SAR immediately, they may result in or contribute to a SAR down the road. Therefore, it's a good practice to track all internal reports and their disposition. Obviously, there should be good record-keeping and security controls over the case tracking system. While making the investment, the system should also provide flexible database management and meaningful reporting. Auditors should review the case tracking mechanism and identify any control deficiencies and opportunities for improvement.

Compliance Monitoring and Assessment

The BSA requirement for a strong monitoring function applies squarely to SAR programs where applicable. Auditors should review the compliance review, assessment, or monitoring program (different terms are used from business to business) to make sure that this requirement is being adequately addressed. Compliance assessment is the primary mechanism through which the compliance function can assess the quality and effectiveness of the SAR program in place. The auditor should determine whether or not this program is in place and whether qualified professional staff is performing periodic assessment, and the results being reported and acted upon.

Confidentiality and Security

While virtually everyone has KYC and event reporting roles and responsibilities, far fewer will play a role in subsequent investigation, analysis, determination, tracking and ultimate SAR reporting. For very compelling reasons, not the least of which are confidence, the risk of tipping off, safety, and safe harbor, strong controls surrounding sar process flow, recordkeeping and reporting are critical. In reviewing the overall sar process, the auditor should review controls in place and should test them to see that they are functioning as designed. This includes testing to make sure that SARs don't leave the "four walls" of the enterprise, except for those filed with law enforcement through proper channels.

The auditor should consider another important aspect of confidentiality – the ability for employees to make confidential reports of unusual or suspicious activity directly to designated compliance officials. This ability requires well-defined channels of access and communication, e.g. an employee hot line.

Information and Communication

Also consistent with the Profession's COSO methodology, the auditor should examine and assess the quality of strategic, compliance and operational information surrounding and driving the sar process and the adequacy of the channels of communication.

Enabling and strengthening the program elements and practices described above require quality information, information processing, and well-defined and working channels of communication to be effective. The sar and SAR flows themselves as well as management information regarding program performance, risk assessment and response has to be accurate, meaningful and timely to enable senior management to make well-informed decisions governing the sar process. Assessing the quality of information and information processing connected with the operational sar process itself may require some in-depth analysis. This will likely include assessing the timeliness, accuracy, efficiency, effectiveness, quality and usefulness of the mechanisms, reports and reporting tools used by designated employees to support the monitoring, escalation, investigation, analysis and reporting of unusual and suspicious activity. Here it may be prudent to assign an IT auditor to look at the automated processes. (However, don't loose sight of the total quality process surrounding the production and flow of information inherent in the other SAR program criteria — the technology tools in place are only at least as effective as the human processes that drive and respond to them).

Similarly, the auditor needs to identify the channels of communication surrounding the sar process and evaluate their effectiveness. Channels should and conventionally include: internal conveyances of written compliance program (usually email, web-site postings and employee manuals, compliance and business unit meetings, training and awareness sessions, and "kitchen posters (e.g. "Do You Know Suspicious Activity When You See It?)"

Section 8 – Mailbag and Feedback

FinCEN is keenly interested in hearing from financial institutions about the value and meaning of *The SAR Activity Review – Trends, Tips and Issues and By The Numbers* to their daily operational and compliance needs. Since the first issue in October 2000, a feedback form has been included with each edition to enable members of the financial community and others to provide comments, suggestions, and other information about the usefulness of the information contained therein. The feedback form has undergone a metamorphosis from a very simple form in Issue 1, to a "rating" form in Issues 2 through 5, and finally to an issue specific form, which appears on the following three pages in this edition. Unfortunately, after the publication of Issue 5 in February 2003, only a few financial institutions provided feedback to FinCEN.

Please, when you have completed digesting all the information contained in this issue of *The SAR Activity Review*, take a few moments to complete and return the Feedback form. As the Introduction states, the continuing exchange of information is critical to improve the SAR system. Your help is wanted and needed in this effort.

Financial Crimes Enforcement Network
Department of the Treasury

Your feedback is important and will assist us in planning future issues of ***The SAR Activity Review****. Please take the time to complete this form. Thank you for your cooperation.*

A. Please identify your type of financial institution.

Depository Institution:
__ Bank or Bank Holding Company
__ Savings Association
__ Credit Union
__ Edge & Agreement Corporation
__ Foreign Bank with U.S. Branches or Agencies

Securities and Futures Industry:
__ Securities Broker/Dealer
__Futures Commission Merchant
__Introducing Broker in Commodities
__Mutual Fund

Money Services Business:
__ Money Transmitter
__ Money Order Company or Agent
__ Traveler's Check Company or Agent
__ Currency Dealer or Exchanger
__ U.S. Postal Service

Casino or Card Club
__ Casino located in Nevada
__ Casino located outside of Nevada
__ Card Club

Other (please identify): _____

B. Please indicate your level of satisfaction with each section of this issue of *The SAR Activity Review- Trends Tips and Issues* (circle your response).
1=Not Useful, 5=Very Useful

Section 1 - Trends and Analysis	1	2	3	4	5
Section 2 - Other Analysis & Examples	1	2	3	4	5
Section 3 - Law Enforcement Cases	1	2	3	4	5
Section 4 - Tips on SAR Form Preparation & Filing	1	2	3	4	5
Section 5 - Issues & Guidance	1	2	3	4	5
Section 6 – SAR News Update	1	2	3	4	5
Section 7 - Industry Forum	1	2	3	4	5
Section 8 – Mailbag and Feedback	1	2	3	4	5

C. What information or article in this edition did you find the most helpful or interesting? Please explain why (please indicate by topic title and page number):

_____
_____
_____
_____
_____
_____

D. What information did you find least helpful or interesting? Please explain why (again, please indicate by topic title and page number):

_____

_____

E. Did you find the new Index Listing of Previous and Current SAR Topics useful?

Yes No

F. Do you like the new delivery format of bifurcating *The SAR Activity Review* into two companion products?

Yes No

Please explain why or why not:

_____

_____

G. Do you plan to review and/or use *The SAR Activity Review – By the Numbers*?

Yes No

How will you use the statistical data in *By the Numbers*?

_____

_____

What other statistical data would you find interesting or useful?

_____

_____

H. What new trends or patterns in suspicious activity would you like to see addressed in the next edition of *The SAR Activity Review – Trends, Tips and Issues*? Examples might include: in a particular geographic area; concerning a certain type of transaction or instrument; other hot topics, etc.

_____

_____

I. What topics would you like to appear in the next or future editions of *The SAR Activity Review – Trends, Tips and Issues?*

_____

_____

J. What questions does your financial institution have about *The SAR Activity Review*, which you would like to have answered?

_____

_____

K. Which of the previous issues have you read? (Check all that apply)

[ ] October 2000 [ ] June 2001 [ ] October 2001 [ ] August 2002 [ ] February 2003

Send your Feedback Form to:

Nona S. Tiedge
FinCEN
Office of Strategic Analysis
Fax 703-905-3698
tiedgn@fincen.treas.gov

Appendix

Index of Topics From Current and Previous Issues of *The SAR Activity Review*

Topic	Issue	Page	Hyperlink Address to *SAR Activity Review* Issue
Automobile Retail Industry: SAR Analysis – Indications of Suspicious Activity	5	27	http://www.fincen.gov/sarreviewissue5.pdf
Boat/Yacht Retail Industry: SAR Analysis – Indications of Suspicious Activity	5	31	http://www.fincen.gov/sarreviewissue5.pdf
Computer Intrusion	3	15	http://www.fincen.gov/sarreviewissue3.pdf
Correspondent Accounts and Shell Company Activity	2	18	http://www.fincen.gov/sarreview2issue4web.pdf
Coupon Redemption Fraud	6	14	http://www.fincen.gov/sarreviewissue6.pdf
Credit/Debit Cards: Suspicious Activity	4	29	http://www.fincen.gov/sarreview082002.pdf
Egmont Group- Strategic Analysis Initiative	2	24	http://www.fincen.gov/sarreview2issue4web.pdf
FATF Typologies Exercise	2	23	http://www.fincen.gov/sarreview2issue4web.pdf
Global Use of SARs	2	24	http://www.fincen.gov/sarreview2issue4web.pdf
Index of Topics from Previous SAR Activity Review Issues	6	85	http://www.fincen.gov/sarreviewissue6.pdf
Identity Theft	2	14	http://www.fincen.gov/sarreview2issue4web.pdf
Identity Theft – Update	3	24	http://www.fincen.gov/sarreviewissue3.pdf
Increased SAR Reporting Involving Mexico	1	12	http://www.fincen.gov/sarreviewforweb.pdf
Indicators of Misuse of Informal Value Transfer Systems	5	18	http://www.fincen.gov/sarreviewissue5.pdf
Industry Forum: Check Fraud Loss Report	5	69	http://www.fincen.gov/sarreviewissue5.pdf
Industry Forum: Check Fraud Loss Report	1	29	http://www.fincen.gov/sarreviewforweb.pdf
Industry Forum: Questions and Answers on MSBs	2	38	http://www.fincen.gov/sarreview2issue4web.pdf
Industry Forum: Some Tips for Auditing the Suspicious Activity Reporting Program	6	71	http://www.fincen.gov/sarreviewissue6.pdf
Industry Forum: Recommended Security Procedures for Protecting Customer Information	3	45	http://www.fincen.gov/sarreviewissue3.pdf
Industry Forum: Safe Harbor Protection for Employment References	4	53	http://www.fincen.gov/sarreview082002.pdf
Issues and Guidance: Advanced Fee Schemes	4	49	http://www.fincen.gov/sarreview082002.pdf
Issues and Guidance: Applicability of Safe Harbor	3	44	http://www.fincen.gov/sarreviewissue3.pdf
Issues and Guidance: Applicability of Safe Harbor	2	37	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: BSA Guidance – IRS Computing Center / FinCEN Help Line & Website	6	65	http://www.fincen.gov/sarreviewissue6.pdf

Issues and Guidance: Cessation of Relationship/Closure of Account	1	27	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: Disclosure of SAR Documentation	2	36	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Disclosure of SARs and Underlying Suspicious Activity	1	28	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: FAQs from FinCEN Help Line – 314a Process	6	59	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: FAQs from FinCEN Help Line – MSB SAR Reporting Questions	6	61	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Filing SARs on Activity Outside the United States	2	35	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Filing SARs on Continuing Activity after Law Enforcement Contact	2	35	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Filing SARs on OFAC List or 314(a) Matches	6	64	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Financial Institutions Hotline	3	43	http://www.fincen.gov/sarreviewissue3.pdf
Issues and Guidance: Florida Appeal Court Decision re: SAR production	6	65	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Office of Foreign Assets Control (OFAC)	4	49	http://www.fincen.gov/sarreview082002.pdf
Issues and Guidance: PATRIOT Act Communications System	5	65	http://www.fincen.gov/sarreviewissue5.pdf
Issues and Guidance: Prohibition on Notification	2	36	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Repeated SAR Filings on Same Activity	1	27	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: SAR Disclosure as part of Civil Litigation	4	50	http://www.fincen.gov/sarreview082002.pdf
Issues and Guidance: SAR Rulings: SAR Disclosure	5	66	http://www.fincen.gov/sarreviewissue5.pdf
Issues and Guidance: Timing for SAR filings	1	27	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: USA PATRIOT Act: 314(a) Information Requests	5	66	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Black Market Peso Exchange	2	28	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Bankruptcy Bust-out Scheme	6	42	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Bankruptcy Fraud Involving Family Members	6	41	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Check Cashing Business	3	34	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Check Kiting Suspect	2	29	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Cocaine Trafficker	2	30	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Computer Chip Theft Ring	3	33	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Conviction of Pharmacist	5	54	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Counterfeit Check Fraud	1	17	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Credit Card Theft	2	30	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Criminal Organization - Baby Formula	1	18	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Customs Fraud	1	17	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Drug Money Laundering	1	22	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Drug Trafficking and Money Laundering	2	29	http://www.fincen.gov/sarreview2issue4web.pdf

Law Enforcement Case: Embargo Investigation	2	28	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Embezzlement	1	16	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Extortion and Title 31	3	29	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Food Bank Theft	1	19	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Forgery of U.S. Treasury Checks	6	44	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Former Banker Sentenced for Avoiding IRS Reporting	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Hawala Investigation	6	38	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Illegal Casa de Cambio	3	34	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Illegal Money Transfers to Iran	5	51	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Illegal Money Transfers to Iraq	4	35	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Importance of SAR Reporting to Law Enforcement Investigations	3	37	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Internal Fraud at Local Bank	5	54	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: International Money Laundering Case	4	36	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Investment Firm CEO	5	53	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Investment Fraud Scheme	6	43	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Investment Fraud Scheme	1	16	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Investment Scam	3	30	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Medicaid Fraud	1	22	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Metal Traders Charged in International Bank Fraud Scheme	4	36	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Methamphetemine Production Ring	3	31	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Money Laundering by RV Dealer	3	30	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Money Laundering in Maryland	4	39	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Money Laundering involving Insurance Industry	5	53	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Money Laundering involving Iraq	6	39	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Money Laundering of Marijuana Sales Proceeds	6	44	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Money Remitter Sending Money to Iraq	5	52	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Nigerian Advance Fee Scam	6	40	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Operation Mule Train	1	18	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Organized Crime Network	1	18	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Phantom Bank Scheme	2	30	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Ponzi Schemes	2	26	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Securities Dealer	2	28	http://www.fincen.gov/sarreview2issue4web.pdf

Law Enforcement Case: Sports Betting Ring	3	31	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Sports Card Theft	3	32	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Stock Fraud	1	21	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Stolen Check Ring	3	32	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Stolen Check Scheme	2	31	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Structuring and Food Stamp Fraud	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Structuring by Three Family Members	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Tax Evasion Case	4	38	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Travel Agent	2	29	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Unlicensed Money Remitter ($1.2 million)	6	40	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Unlicensed Money Remitter ($3 million)	5	52	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Unlicensed Money Remitter ($427,000)	5	51	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Unlicensed Money Transmission Scheme	4	35	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Worker's Compensation Fraud	1	20	http://www.fincen.gov/sarreviewforweb.pdf
Life Insurance: SAR Analysis – Indications of Suspicious Activity	5	35	http://www.fincen.gov/sarreviewissue5.pdf
Mailbag and Feedback	6	79	http://www.fincen.gov/sarreviewissue6.pdf
Mailbag – Questions from the Industry	3	49	http://www.fincen.gov/sarreviewissue3.pdf
Money Services Businesses: SARs filed by MSBs	4	33	http://www.fincen.gov/sarreview082002.pdf
Money Transmitter Activity	2	18	http://www.fincen.gov/sarreview2issue4web.pdf
Money Transmitters may be Money Laundering Vehicle	3	17	http://www.fincen.gov/sarreviewissue3.pdf
Multilateral Illicit Currency Flows Study	2	23	http://www.fincen.gov/sarreview2issue4web.pdf
Non-Cooperative Countries and Territories	3	27	http://www.fincen.gov/sarreviewissue3.pdf
Non-Cooperative Countries and Territories	2	22	http://www.fincen.gov/sarreview2issue4web.pdf
Non-Cooperative Countries and Territories	1	15	http://www.fincen.gov/sarreviewforweb.pdf
On-line and/or Internet Banking	6	27	http://www.fincen.gov/sarreviewissue6.pdf
Pawn Brokers: SAR Analysis – Indications of Suspicious Activity	5	33	http://www.fincen.gov/sarreviewissue5.pdf
Percentage of SARs Reporting Structuring	3	25	http://www.fincen.gov/sarreviewissue3.pdf
Pre-paid Telephone Cards	2	19	http://www.fincen.gov/sarreview2issue4web.pdf
Real Estate Industry – Sales and Management SARS	6	31	http://www.fincen.gov/sarreviewissue6.pdf
Regional Money Remitter Activity	1	13	http://www.fincen.gov/sarreviewforweb.pdf
Reports of Solicitation Letters (Advanced Fee Fraud or 4-1-9 Scams)	3	23	http://www.fincen.gov/sarreviewissue3.pdf
Role of SARs in High Risk Money Laundering and Related Financial Crime Areas	1	14	http://www.fincen.gov/sarreviewforweb.pdf

Russian Criminal Activity	1	12	http://www.fincen.gov/sarreviewforweb.pdf
SAR News Update: Expansion of PACS	6	67	http://www.fincen.gov/sarreviewissue6.pdf
SAR News Update: Expansion of SAR and AML Compliance Requirements to New Industries	4	46	http://www.fincen.gov/sarreview082002.pdf
SAR News Update: Expansion of SAR Requirements to New Industries	5	61	http://www.fincen.gov/sarreviewissue5.pdf
SAR News Update: Financial Industries Required to File SARs	6	69	http://www.fincen.gov/sarreviewissue6.pdf
SAR News Update: FinCEN's Financial Institutions Hotline	4	45	http://www.fincen.gov/sarreview082002.pdf
SAR News Update: Non-Cooperative Countries and Territories	6	68	http://www.fincen.gov/sarreviewissue6.pdf
SAR News Update: Proposed Revision to Suspicious Activity Report	5	62	http://www.fincen.gov/sarreviewissue5.pdf
SAR News Update: USA PATRIOT Act: Section 311 Authority	5	62	http://www.fincen.gov/sarreviewissue5.pdf
SAR News Update: USA PATRIOT Act 314a Project Progress Report	6	37	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: Computer Intrusion and Frequently Asked Questions	3	38	http://www.fincen.gov/sarreviewissue3.pdf
SAR Tips: Filing a Corrected or Amended SAR	4	42	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: Filing a SAR for Ongoing or Supplemental Information	4	43	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: Identity Theft and Pretext Calling	3	41	http://www.fincen.gov/sarreviewissue3.pdf
SAR Tips: Importance of Accurate and Complete Narratives	5	55	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Importance of the Narrative	2	32	http://www.fincen.gov/sarreview2issue4web.pdf
SAR Tips: Improvements to Eliminate Reporting Deficiencies	6	49	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: Informal Value Transfer System--Special SAR Form Completion Guidance	5	57	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Instructions for Completing the SAR Form	6	50	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: SAR Filing Tips for MSBs	4	42	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: SAR Form Completion Rate-National Overview	1	25	http://www.fincen.gov/sarreviewforweb.pdf
SAR Tips: SAR Form Preparation and Filing	1	24	http://www.fincen.gov/sarreviewforweb.pdf
SAR Tips: SAR Forms: Where to Send Completed SAR Forms	5	58	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: SAR Forms: Where to Send Completed SAR Forms	6	57	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: Special Guidance Related to Identity Theft and Pretext Calling	2	34	http://www.fincen.gov/sarreview2issue4web.pdf
SAR Tips: Terrorist-Related Activity: How to report potential terrorist-related activity	6	53	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: Terrorist-Related Activity: How to report potential terrorist-related activity	5	55	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Terrorist-Related Activity: How to report potential terrorist-related activity	4	41	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: Tips from the Regulators	6	54	http://www.fincen.gov/sarreviewissue6.pdf
SARs filed by Money Services Business	5	48	http://www.fincen.gov/sarreviewissue5.pdf
SARs Filed Referring to Terrorism (Prior to 09/112001 & 09/112001 through 03/31/2002)	4	25	http://www.fincen.gov/sarreview082002.pdf
SARs Filed that Refer to Terrorism (March –September 2002)	5	21	http://www.fincen.gov/sarreviewissue5.pdf

Securities Industry: SAR Analysis – Indications of Suspicious Activity	5	38	http://www.fincen.gov/sarreviewissue5.pdf
Securities and Futures Industries SARs: The First Quarter	6	23	http://www.fincen.gov/sarreviewissue6.pdf
Shell Company Activity	1	11	http://www.fincen.gov/sarreviewforweb.pdf
State and Local Law Enforcement Use of SAR Data	6	45	http://www.fincen.gov/sarreviewissue6.pdf
State and Local Law Enforcement Use of SAR Data	4	39	http://www.fincen.gov/sarreview082002.pdf
State and Local Law Enforcement Use of SAR Data	3	33	http://www.fincen.gov/sarreviewissue3.pdf
Suspicious Activity Reported by Casinos	1	13	http://www.fincen.gov/sarreviewforweb.pdf
Suspicious Automated Teller Machine (ATM) Activity	1	13	http://www.fincen.gov/sarreviewforweb.pdf
Terrorist Financing Methods: Coupon Redemption Fraud	6	14	http://www.fincen.gov/sarreviewissue6.pdf
Terrorist Financing Methods: Hawalas	5	19	http://www.fincen.gov/sarreviewissue5.pdf
Terrorist Financing Methods: Informal Value Transfer Systems	5	17	http://www.fincen.gov/sarreviewissue5.pdf
Terrorist Financing Methods: Informal Value Transfer Systems – Update	6	6	http://www.fincen.gov/sarreviewissue6.pdf
Terrorist Financing Methods: Non-Profit Organizations	5	21	http://www.fincen.gov/sarreviewissue5.pdf
Terrorist Financing Methods: SAR Filers Identify Suspicious Monetary Instruments Clearing Through International Cash Letters	6	12	http://www.fincen.gov/sarreviewissue6.pdf
Terrorist Financing: Aspects of Financial Transactions that May Indicate Terrorist Financing	4	17	http://www.fincen.gov/sarreview082002.pdf
Terrorist Financing: Financial Action Task Force (FATF) Efforts	4	27	http://www.fincen.gov/sarreview082002.pdf
Terrorist Financing: FinCEN Analysis of SAR Filings and other BSA information	4	19	http://www.fincen.gov/sarreview082002.pdf
Terrorist Financing: Reconstruction of Hijacker's Financial Activities	4	18	http://www.fincen.gov/sarreview082002.pdf
Terrorist Financing: Terrorism and Terrorist Financing	6	3	http://www.fincen.gov/sarreviewissue6.pdf
Travel Industry: SAR Analysis – Indications of Suspicious Activity	5	25	http://www.fincen.gov/sarreviewissue5.pdf
Use of Traveler's Checks to Disguise Identities	3	22	http://www.fincen.gov/sarreviewissue3.pdf
Voluntary SAR Filings	3	26	http://www.fincen.gov/sarreviewissue3.pdf
Voluntary SAR Filings	2	19	http://www.fincen.gov/sarreview2issue4web.pdf