The SAR Activity Review

Trends

Tips &

Issues

Issue 7

August 2004

The SAR Activity Review

Trends

Tips &

Issues

Issue 7

Published under the auspices of the Bank Secrecy Act Advisory Group

August 2004

Table of Contents

Section 3 - Tips on Suspicious Activity Report Preparation and Filing

Section 4 - Issues and Guidance

Section 5 - Industry Forum

Section 6 - Mailbag and Feedback

Appendix – Index of Topics from Current and Previous Editions of *The SAR Activity Review – Trends, Tips & Issues*

Introduction

The SAR Activity Review-Trends, Tips & 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 filed by financial institutions.

Many of the topics addressed in this issue were selected in response to feedback submitted by financial industries' representatives, regulators, law enforcement agents, and other readers who requested information on trends and patterns in suspicious activity reporting related to specific topics of interest. Significant topics presented in this issue encompass analyses of emerging and traditional money laundering schemes and possible terrorist financing mechanisms, which threaten the integrity and safety of our nation's financial systems.

- Section 1, Trends and Analyses, presents information about the suspected use of United States-based shell corporations and foreign shell banks by some Eastern European criminals to move money through correspondent bank accounts; electronic benefit transfer cards used in food stamp fraud; and suspicious endorsed/third-party checks negotiated abroad and cleared through international cash letters for money laundering, terrorist financing, or other criminal schemes. Additionally, this section provides an analysis of refund anticipation loan fraud; an update on Suspicious Activity Report forms filed by broker-dealers in securities after the first year of mandated suspicious activity reporting; money laundering activities related to the use of automated teller machines to move illicit proceeds; and information about consumer loan fraud.

- Section 2, Law Enforcement Cases, provides an update on the effectiveness of the USA PATRIOT Act Section 314(a) process and also includes cases where Suspicious Activity Report filings were helpful.

1Participants 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 for Terrorist Financing & Financial Crimes (EOTF/FC), Internal Revenue Service (IRS), and the Financial Crimes Enforcement Network (FinCEN).

- Section 3, Tips on Suspicious Activity Report Form Preparation and Filing, presents an explanation of the violation types listed in Item 35 (summary characterization of suspicious activity) on the depository institution Suspicious Activity Report form.

- Section 4, Issues & Guidance, provides guidance for financial institutions on proper procedures to follow when served with a civil subpoena for records that might include any Suspicious Activity Report filings, as well as guidance on reporting advance fee schemes.

- Section 5, Industry Forum, addresses suspicious activity reporting compliance.

- Section 6, Mailbag and Feedback, provides information in response to a request about the Bank Secrecy Act/Structuring/Money Laundering characterization of the suspicious activity category.

Readers are reminded that, as announced in the November 2003, *Issue 6*, the statistical data formerly found in *Issues 1 through 5*, Section One, Suspicious Activity Report Statistics, and in Appendix 1, Characterization of Suspicious Activity by States and Territories by Year, now appears in a companion product, *The SAR Activity Review – By the Numbers*. The second edition of that report was published in May 2004 and is available on the FinCEN website, www.fincen.gov.

All other sections formerly published in *The SAR Activity Review – Trends, Tips & Issues* will be published in the spring and fall. Previous editions were published in October 2000, June 2001, October 2001, August 2002, February 2003, and November 2003. Refer to the Appendix at the end of this Issue to locate specific topics, law enforcement cases, guidance and other information from those previous editions.

Your comments and feedback are important to us. Please take a moment and complete the Feedback Sheet in Section 6 to let us know if the topics chosen for this edition are helpful to you and to suggest future topics. Your comments may be addressed to either or both of *The SAR Activity Review* project co-chairs:

John J. Byrne
Director
Center for Regulatory Compliance
American Bankers Association
1120 Connecticut Ave., NW
(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)
David.Gilles@fincen.gov

Section 1 – Trends and Analysis

FinCEN continues to identify, explore and report on traditional and non-traditional mechanisms used by money launderers, terrorist financiers, and other criminals to move illicit funds through formal and informal financial systems. Terrorist organizations also may use alternative and less obvious means to acquire and move capital. Those means may involve committing crimes that, in the past, were not immediately associated with terrorist fundraising and financing schemes. Examples include coupon redemption fraud, interstate contraband cigarette smuggling, and credit card fraud. The food services industry recognizes their vulnerability to these and other criminal schemes, and is actively working to identify, report and combat abuse. Recent analysis of Suspicious Activity Report forms reporting activities and money generated from certain crimes has identified an emerging set of possibilities for misuse of the financial system by criminal and terrorist organizations. FinCEN will continue a comprehensive study of financial industries' services and products vulnerable to abuse by money launderers, terrorist financiers and criminals.

Use of United States-Based Shell Corporations and Foreign Shell Banks by Eastern Europeans to Move Money

In recent years following the public reporting of a 1999 investigation into questionable Russian-related correspondent banking activities, the publication of a 2000 General Accounting Office report entitled "Possible Money Laundering by U.S. Corporations Formed for Russian Entities,[2]" and the 2001 Senate hearings on the role of United States correspondent banking in international money laundering, there has been an increased focus on the money laundering risks associated with foreign-owned, United States-based shell corporations[3] and foreign shell banks with no presence in the United States other than a bank account. Recent findings by the State of New York Banking Department[4] have noted a steady increase in the number of Suspicious Activity Reports filed by New York banks.[5] These filings report an increase in the volume of shell company wire transfer activity in both dollar

2 See General Accounting Office Report, GAO-01-0120, October 2000, at www.gao.gov

3 The terms, "shell corporation" and "shell company," are used interchangeably in this report.

4 The Department is the primary regulator for state-licensed and state-chartered financial entities, including domestic banks, foreign agencies, branches and representative offices, savings institutions and trust companies and other financial institutions operating in New York including mortgage bankers and brokers, check cashers, money transmitters, and licensed lenders, among others.

5 In the United States, many domestic and international banks, which offer correspondent banking services, maintain their operations centers in New York.

amounts and the number of transactions through high-risk correspondent bank accounts. Specifically, extraordinary sums of money are passing through correspondent accounts established for Eastern European banks. The use of shell corporations and shell banks to launder money and possibly finance terrorist activities is a concern shared by government financial intelligence units worldwide. In light of the continuing concerns about foreign shell banks, in October 2001, the Congress included provisions in Title III of the USA PATRIOT Act to prohibit correspondent accounts for foreign shell banks.

Recently, FinCEN conducted a preliminary analysis of Suspicious Activity Report filings of suspicious activities involving foreign shell banks, specifically those in Eastern European countries, to determine trends and patterns in transactions before and after enactment of Section 313 and Section 319 of the USA PATRIOT Act (Public Law 107-56).

Shell Corporations

Shell corporations are described as companies with no independent assets or operations of their own, which are used by their owners to conduct business dealings or maintain control of other companies. A shell corporation is registered or licensed in the state or country in which it is incorporated or established, is not traded on a securities exchange, and does not operate on its own. While shell corporations are not illegal or improper, money launderers, tax evaders and terrorist financiers have used shell corporations as a means to disguise the illicit nature of their money. They are easily established and can be interlocked with other shell corporations located all over the world. If a shell corporation is established in a jurisdiction with strict secrecy laws, it can be almost impossible to identify the owners or directors of the corporation and therefore nearly impossible to trace illicit funds back to their true owner. This is precisely the effect the launderer, terrorist financier and tax evader seeks, and is why shell corporations are an effective means of interrupting the paper trail used by investigators.[6]

Shell corporations typically exist only on paper. The corporation's formation documents may list a valid bank account and little more than the name and address of the lawyer or agent handling the incorporation, some officers, and perhaps a few shareholders. When criminals seek to utilize shell corporations to disguise ownership or other illicit activity, they will provide fictitious names or nominee names on the corporate formation documents. These accounts play very important roles in illicit money movements because they can be used to receive deposits and as transfer points to the accounts of other shell corporations, legitimate businesses or individuals. The incorporation documents give shell corporations the outward appearance of legitimate businesses, allowing their bank accounts to be used to receive structured cash deposits designed to avoid currency reporting requirements.

---

6 Shell company activity has been a topic in previous issues of *The SAR Activity Review*. For additional information, refer to Issue 1 (pages 11-12) and Issue 2 (page 18).

A review of Suspicious Activity Report data indicates that suspected shell corporations, like legitimate businesses, appear to establish customer relationships with financial institutions in other countries around the world—many of which are located in Eastern European countries.

- 397 Suspicious Activity Reports filed between April 1996 (the time financial institutions were mandated to file Suspicious Activity Reports) and January 2004 involved *shell corporations, Eastern European countries,*[7] and the *use of correspondent bank accounts*. The aggregate violation amount reported in those 397 Suspicious Activity Report forms totaled almost $4 billion.

Many of these financial institutions, in turn, had established correspondent banking relationships with financial institutions in the United States.[8]

USA PATRIOT Act Provisions

As required by §313(a) and §319(b) of the USA PATRIOT Act, on September 26, 2002, FinCEN published a final rule at 67 FR 60562, codified in 31 CFR Part 103, addressing an important subset of shell corporations: foreign shell banks. 31 CFR §103.175 defines a foreign shell bank as "a foreign bank without a physical presence in any country." Foreign bank is defined in 31 CFR §103.11(o) as "a bank organized under foreign law," but not including its agents, branches, or offices located in the United States. 31 CFR §103.177 imposes certain responsibilities on banks and broker-dealers operating in the United States if they maintain correspondent accounts for foreign shell banks and foreign banks. Specifically, §103.177 prohibits covered financial institutions from maintaining correspondent accounts for foreign shell banks.[9]

The record-keeping requirements of §103.177 implement the statutory requirement of §319(b) of the USA PATRIOT Act. The portion of §103.177 that implements §319(b) requires covered financial institutions that maintain correspondent accounts for foreign banks to obtain records of the owners of those foreign banks and of their agents who are authorized to accept service of legal process. Section 319(b) is an important tool for regulators and the law enforcement community by allowing them to quickly obtain ownership information about these foreign institutions and identify individuals who can accept legal process when a subpoena for financial records must be served.

---

7 The Eastern European Countries that were identified in Suspicious Activity Report narratives with shell companies included Armenia, Belarus, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Georgia, Greece, Kazakhstan, Latvia, Lithuania, Moldova, Poland, Romania, Russia, Slovenia, Turkey, Turkmenistan, Ukraine, Uzbekistan and Yugoslavia.

8 Correspondent banks hold deposits for other banks and perform banking services for a fee, such as check clearing for banks in other cities or countries. The deposit balance is often a form of payment for services. Correspondent banks also buy participations in loans exceeding the legal lending limit of a smaller bank and give these banks access to financial markets that are ordinarily beyond the reach of smaller financial institutions.

9 For more information see FinCEN Ruling 2003-2.

31 CFR §103.177 requires any covered financial institution that provides a correspondent account for a foreign bank to maintain records of the foreign bank's owners and to maintain the name and address of an agent in the United States that has been designated to accept service of legal process for the foreign bank for records related to the correspondent account. 31 CFR §103.177 requires covered financial institutions to obtain from the foreign bank a certification with certain information,[10] or otherwise obtain documentation of the required information. For correspondent accounts that existed on October 28, 2002, 31 CFR §103.177 requires a covered financial institution to close the correspondent account, within a commercially reasonable time, if the covered financial institution had not received the appropriate certification from the foreign bank, or otherwise obtained documentation of the required information, on or before March 31, 2003.

Suspicious Activity Report Analysis Trends for Foreign Shell Banks

Financial institutions have used Suspicious Activity Report narratives to report their assessment that suspected foreign shell banks have facilitated the movement of monies through the financial systems in the United States on behalf of alleged account holders. Domestic banks reported they were able to verify incorporation in this country for corporate entities related to possible foreign shell bank operations, but were unable to identify corporate physical locations, ownership, officers or directors. Prior to the adoption of 31 CFR §103.177, financial institutions filed Suspicious Activity Reports with narratives describing instances of foreign shell banks allegedly operating as unlicensed banks in the United States and moving funds through domestic correspondent accounts to accounts in foreign countries. After 31 CFR §103.177 was adopted, no Suspicious Activity Report filings indicate foreign shell banks operating in the United States. Ostensibly, banks would have closed these accounts to comply with the regulation. However, what financial institutions in the United States describe in some Suspicious Activity Reports as possible foreign shell banks continue to indirectly route account holders' funds through United States correspondent accounts. Suspicious Activity Reports also reported activity conducted by alleged foreign shell banks through foreign banks' correspondent accounts with institutions in the United States (those institutions were acting as intermediary banks.) According to regulation, domestic financial institutions must take reasonable measures to ensure that any correspondent account they establish, maintain, administer, or manage for a foreign bank is not being used by the foreign bank to provide banking services indirectly to a foreign shell bank.[11]

Queries by FinCEN analysts of the database housing Suspicious Activity Reports revealed some interesting facts.

10 See Appendix A to Subpart I of 31 CFR Part 103 – "Certification Regarding Correspondent Accounts for Foreign Banks" [OMB Control Number 1505-0184].

11 See 31 CFR 103.177(a)(1)(ii).

- For the period April 1996 through January 2004, 71 Suspicious Activity Reports were filed that identified activities involving *foreign shell banks*. Those 71 Suspicious Activity Reports reported an aggregate suspected violation amount of almost $500 million.

- Prior to December 26, 2002, the initial effective date of 31 CFR Part 103.177, there were 30 Suspicious Activity Reports that reported suspicious activity involving alleged *Eastern European*[12] *shell banks* and the *use of correspondent accounts*. This represents a monthly average of less than one Suspicious Activity Report.

- 41 Suspicious Activity Reports were filed after the final rule's December 26, 2002 effective date, with the most recent Suspicious Activity Report filed October 3, 2003.[13] The monthly average over this 13-month period (January 2003-January 2004) was 3.2 Suspicious Activity Reports, not a significant increase, but an increase nevertheless.

- The current rule extended the time for obtaining certain information concerning correspondent accounts from December 26, 2002 to March 31, 2003. During this three-month period (January-March 2003), a total of 24 Suspicious Activity Reports were filed, representing 8 Suspicious Activity Reports per month, considerably higher than before the regulation was adopted.

As noted above, financial institutions have reported and continued to report through October 2003, correspondent account activities involving suspected shell corporations and foreign shell banks in Suspicious Activity Report narratives.

Indicators of Possible Misuse of Shell Corporations and Shell Banks

Based on the activity reported in Suspicious Activity Reports, financial institutions should be alerted to the following red flags regarding shell companies and shell banks. Taken individually these indicators may not point to suspicious activities relating to shell companies or shell banks. However, used in combination with the definitions provided for shell corporations, these indicators may arouse suspicions.

- An unusually high volume of wire transfer activity with multiple wire transfers totaling hundreds or thousands and with dollar amounts in the thousands or millions. These wires frequently involve originators located in high-risk regions considered vulnerable to money laundering.

---

12 The Eastern European Countries that were identified in Suspicious Activity Report narratives with shell banks included Bulgaria, Cyprus, Estonia, Georgia, Kazakhstan, Latvia, Lithuania, Poland, Russia, Turkey, Ukraine and Yugoslavia.

13 As of January 2004.

- Payment originators with addresses in the United States but who originate the payments from accounts held at foreign banks.

- Inability to identify a location in the United States, corporate officers and/or directors or the nature of the business.

- Suspected shell companies based in foreign countries, which are customers of foreign banks that maintain correspondent accounts with United States-based banks. The shell companies, through the correspondent accounts, wire funds to offshore jurisdictions.

- Foreign-owned corporations based in the United States as originators or beneficiaries (or both) of dollar denominated wire transfers.

- Numerous and large-amount wire transfers sent from offshore jurisdictions through correspondent accounts held at United States-based banks to a foreign bank and then on to a customer's shell corporation.

- Repetitive wire transfers from a particular originator to a particular beneficiary, with one of the parties being a registered corporation in the United States for which no physical location can be identified; the other party is located offshore.

- Individual wire transactions conducted in large, even-dollar amounts.

- Individual wire transactions conducted within a short period of time (i.e. daily basis, two times daily or every other day).

- Unusually large numbers of wire transfers involving offshore correspondent account holders or domestic companies that do not appear to maintain an operating business in the state of incorporation and for which there is no indication of legitimate business activity.

What to do if Suspicious Activity is Suspected

If a financial institution discovers suspicious activities such as those listed above and knows, suspects or has reason to suspect the transactions involve the use of United States-based shell corporations and/or foreign shell banks to launder illicit funds or to enable the furtherance of a crime, the institution must file a Suspicious Activity Report in accordance with the suspicious activity reporting regulations and use the narrative to completely and sufficiently describe the suspicious conduct. It is particularly beneficial to utilize the term "shell" when referencing this type of activity in the Suspicious Activity Report narrative. The preparer should provide all required and relevant information about the conductor(s) and transactions, including the names and account numbers of all originators and beneficiaries of domestic and international wire transfers, the names and locations of legitimate or shell

banks involved in the transfers, and the names and information of any registered agent.

FinCEN will continue to examine Suspicious Activity Report forms reporting suspicious activities through United States-based foreign shell corporations and foreign shell banks to identify vulnerabilities for money laundering, terrorist financing and other financial crimes.

Food Stamp Fraud Using Electronic Benefit Transfer Cards

The United States Department of Agriculture (USDA)[14] Food Stamp Program is the government's primary food assistance program available to help low-income individuals and families obtain nutritious food for healthy diets. In fiscal year 2003, $21 billion in food stamp benefits were issued. The USDA Food and Nutrition Service administers the Food Stamp Program through 53 State government agencies who contract with transaction processing companies for Electronic Benefit Transfer systems.[15] Once an eligible household is approved to receive food stamp benefits, the household is issued an electronic benefit transfer card that is essentially a debit card for purchasing food. A monthly allotment of food benefits averaging about $85 per person is made available to each eligible household at the beginning of each month.

Food stamp recipients can use their benefits to purchase food at licensed stores. There are currently 145,000 stores in the program. The food stamp recipient selects the food to be purchased and goes to the checkout counter at a retail store authorized by the USDA Food and Nutrition Service to accept food stamp benefits. The eligible recipient swipes the Electronic Benefit Transfer card through an electronic point of sale device, and then enter a personal identification number. The information is transferred to the processing facility to determine the validity of the Electronic Benefit Transfer card, the level of available food stamp benefits, and whether or not the retailer is authorized by the Food and Nutrition Service.

Some food stamp recipients, however, sell their Electronic Benefit Transfer cards for cash for less than face value. This activity is known as food stamp trafficking. The authorized retailer processes the Electronic Benefit Transfer card transaction but, in most cases, no food is sold during the trafficking transaction.

14 Some information appearing in this section was prepared and submitted by the United States Department of Agriculture

15 Before the advent of Electronic Benefit Transfer transactions, the Food Stamp Program was administered with engraved paper coupons that were deposited into the authorized retailers' bank accounts. Currently, 96% of the program is being issued through the use of Electronic Benefit Transfer transactions. Please refer to the Food and Nutrition Service website: at http://www.fns.usda.gov/fsp/ebt/ and http://www.fns.usda.gov/fsp/ebt/state_ebt_websites.htm for additional information on the United States Food Stamp Program.

Under either scenario, Electronic Benefit Transfer transactions are reconciled each day and an Automated Clearing House transaction moves the funds from the United States Department of the Treasury to the retailers' bank accounts.

As part of administering the program, the Food and Nutrition Service monitors authorized retailers and Electronic Benefit Transfer transactions to identify suspicious or illegal activity. The Food and Nutrition Service may use Electronic Benefit Transfer transaction records to initiate further investigation of retailers or to take administrative action against them. Information is also provided to the USDA's Office of Inspector General for possible criminal investigation.

An estimated $395 million of food benefits are diverted each year from their intended purpose through food stamp trafficking and associated money laundering activities to hide the illegal proceeds.[16] Law enforcement efforts by the USDA Office of Inspector General and other investigative agencies have linked food stamp trafficking to narcotics trafficking, money laundering, and the transfer of money overseas. Violations and enforcement of the food stamp program are pursued under the provisions of 7, U.S.C. §2024. More information about food stamp trafficking is contained in the USDA Inspector General's Semiannual Reports to Congress found at http://www.usda.gov/oig/rptssarc.htm.

Financial institutions are in a unique position to help the Food and Nutrition Service and law enforcement agencies by identifying suspicious activities related to the Food Stamp Program. Over the years, many financial institutions have played a key role in noting a variety of suspicious activities.

FinCEN found 352 Suspicious Activity Reports filed during the last eight years related to possible food stamp fraud. Examples include the following.

- Financial institutions reported that several food stores received large volumes of food stamp-related electronic credits and executed other suspect financial transactions, mainly cash withdrawals, that are not customary for small food stores.

- Suspicious Activity Reports were filed by numerous banks on food marts where the only funds credited to accounts originated from food stamp Electronic Benefit Transfer transactions. In some instances, these credits were withdrawn from the account through structured cash withdrawals shortly after being credited to the account.

- A Suspicious Activity Report was filed on a cash-intensive food store that processed large food stamp Electronic Benefit Transfer transactions. When

16 Macaluso, Theodore. *The Extent of Trafficking in the Food Stamp Program*. Alexandria, VA: Food and Nutrition Service, 2003.

the food store business account was credited for the Electronic Benefit Transfer activity, agents of the company conducted several structured cash withdrawals from the account. The structuring was done by using different bank branches and executing withdrawals just under $10,000.

- A financial institution filed a Suspicious Activity Report on a food store for possible Bank Secrecy Act/Structuring/Money Laundering violations. The Suspicious Activity Report identified Electronic Benefit Transfer deposits that were credited to the business' account and then followed by cash withdrawals. The withdrawals were usually conducted the day after Electronic Benefit Transfer credits were posted to the account. In addition, checks drawn on the business account were made payable to cash.

- A Suspicious Activity Report identified a small food market receiving food stamp electronic credits. After deposits were received, the filer noted a pattern of suspicious withdrawals made by the storeowner. The storeowner typically requested $1,000 to $5,000 withdrawals in new $100 bills.

- Another Suspicious Activity Report identified a grocery store owner who received Electronic Benefit Transfer funds for food stamp sales to his business account. The Suspicious Activity Report reported structured check cashing that was under federal reporting threshold requirements. The filer noted that the store cashed a large volume of checks. The owner brought those cashed checks to his bank and exchanged them for cash (possibly utilizing third-party endorsement of the instruments).

- A Suspicious Activity Report was filed on a cash intensive business that received numerous food stamp electronic benefit transfers. On a daily basis, agents and associates of the business withdrew funds and cashed checks for just under $10,000 at the business. Some of the checks were made payable to "cash" while others were made payable to unrelated third parties.

As noted above, the bulk of activity involving the Food Stamp Program offers a valuable service for the low-income segment of the population. Moreover, the food and grocery industry has taken a firm stand against all such crimes that abuse the food sales industry. A review by FinCEN of the Suspicious Activity Reports filed by financial institutions indicated several vulnerabilities of the Electronic Benefit Transfer program that may be indicators of abuse of the Food Stamp Program.

Suspicious Endorsed/Third-Party Checks Negotiated Abroad

In Issue 6 of *The SAR Activity Review – Trends, Tips & Issues*, information was provided about monetary instruments negotiated abroad by suspected money

launderers or other criminals and then cleared through international cash letters.[17] FinCEN is continuing to study these activities to identify and report vulnerabilities in the international cash letter process. The information that follows describe another type of instrument cleared through cash letters and used in money laundering schemes: the endorsed/third-party check.

An endorsed/third-party check is a check payable to someone other than the drawer who in turn transfers the check to a third party by endorsing the back of the instrument by writing "pay to the order of" to name a new holder. This action transfers the instrument to a new holder who has the same legal rights as the endorser. The new holder of the instrument is then free to negotiate the check themselves, either by endorsing the check and depositing it into an account, or by exchanging it for cash at a financial institution (bank, money services business, hawala or other type of alternative remittance or underground banking system, etc.) The Uniform Commercial Code allows the transfer of one check to a new owner any number of times.

Many individuals, small businesses, and even some large enterprises have legitimate reasons for using third-party checks for their transactions, particularly in parts of the world where the financial services infrastructure is not as developed as it is in the United States and where there is high demand for the U.S. dollar. At the same time, there is a potential for abuse. Endorsed third-party checks have been used to commit fraud, money laundering, tax evasion and other criminal offenses in the United States and abroad. For example, such checks are commonly used in the black market peso exchange and in other currency black markets in the Middle East, Africa, and the Americas. Such practices are commonly encountered in cases that involve a range of criminal activities. For these reasons, as well as the risk of non-payment, the practice of accepting endorsed/third-party checks is avoided by many financial institutions overseas and even discouraged or disallowed in some jurisdictions. Similarly, when money exchange companies or other financial institutions accept endorsed checks, they often charge a commission of three to five percent to cover the risk of non-payment. In other cases, third-party checks may be accepted for collection only, which delays the payment for several business days.

Suspicious Activity Report narratives have indicated that U.S.-dollar third-party checks are being presented to banks located overseas, even though both the payee and payer appear unconnected to the area where these checks appear. Once negotiated, though, the checks become part of the international cash letter package sent to correspondent banks in the United States. Some of these third-party checks negotiated abroad and sent through the cash letter process might indicate one or more of the following crimes:

17 See Issue 6 of *The SAR Activity Review – Trends, Tips & Issues*, November 2003, pages 12-14, at http://www.fincen.gov/sarreviewissue6.pdf.

- money laundering;
- black market currency deals;
- payment for smuggled or diverted goods;
- tax evasion;
- unlicensed/unregistered hawala/informal fund transfer business or settlement;
- terrorist financing;
- fraud; or
- bribery/corrupt payments.

It is a common practice of financial institutions to flag transactions that make little or no commercial or economic sense. Regulatory authorities encourage this practice as part of a risk-based Bank Secrecy Act compliance program. This does not mean that a single flag proves that illegal activity has been committed, facilitated or covered up through particular checks. Instead, flags alert bank officials and regulators that something may be wrong and that they should exercise due diligence to ensure that their institution does not facilitate illegal activity and does not increase the possibility of reputational, financial or legal risks. In such instances, customer identification programs and banking business rules are particularly useful to avoid these risks.

To assist financial institution employees in preventing and reporting illegal transactions, a non-exhaustive list of possible indicators of endorsed/third-party check abuse is listed below as a guideline. These are some of the suspicious activities identified in Suspicious Activity Report filings for endorsed/third party checks negotiated abroad:

1. Checks payable to payees with no local connection to the city, area, or country where the checks were cashed or deposited (i.e., not payable to a person, organization or business with a local residence, office or business address);

2. Checks for unusually large amounts (i.e. certain threshold amounts, such as $50,000), especially when they appear unrelated to a particular business;

3. Business checks from a bank based in a jurisdiction different from the residence of the payer where there is no apparent connection between the issuer and beneficiary of the check (e.g., an importer in South America pays an exporter in Europe or the United States with a check drawn in the Middle East);

4. Checks written for amounts just below the currency reporting requirement limits ($10,000), which are then cashed out;

5. Checks from a source flagged for previously submitting problematic instruments (e.g., forged signatures, stolen checks, fraudulently obtained checks, suspected money laundering, terrorist finance or other financial crime connected checks);

6. Checks that appear to have no legitimate commercial purpose;

7. Multiple endorsed/third-party checks used for the settlement of a single purchase or transaction;

8. Checks in foreign currency deposited in jurisdictions/areas known to be vulnerable to abuse;

9. Checks on which more than one type of handwriting appears for the original item (e.g., one for the amount and another for the date or payee);

10. Checks in the same name made payable to the same payee, but with different signatures on each check;

11. Checks made out to different payees, but bearing the same handwriting endorsing them;

12. Checks with the payee line left blank;

13. Deposits of multiple endorsed/third-party checks; or

14. Checks dated five or six months before the deposit date.

What to do When Assessing Risk Associated with Foreign Correspondent Accounts and Associated Services

Federal regulatory agencies recommend that banks in the United States exercise caution and due diligence when assessing the risk associated with each of their foreign correspondent accounts and services that are offered through these accounts. For example, the Office of the Comptroller of the Currency has advised the banks it supervises that the level of perceived risk associated with an account relationship, including accessibility of the account by third parties, should dictate how the bank manages the risk.[18] If a financial institution discovers indicators of suspicious activity as described above, a Suspicious Activity Report could be warranted. If a

18 See "High Risk Products and Services / International Correspondent Banking Relationships," p. 21-22, and "Pouch Activity," p. 23-24, in the Office of the Comptroller of the Currency's *Bank Secrecy Act/Anti-Money Laundering Comptroller's Handbook* at www.occ.treas.gov/handbooks/bsa.

Suspicious Activity Report is filed, the narrative should completely and sufficiently describe the suspected activity relating to the use of endorsed/third-party checks by providing information on the parties and accounts involved, the dates, amounts, and account numbers of the checks, and a description of the activity leading the institution to believe the activity is suspicious and therefore causing it to file a Suspicious Activity Report.

Refund Anticipation Loan Fraud

FinCEN, working with the Internal Revenue Service Criminal Investigation's Refund Crimes Section, undertook an in-depth review of refund anticipation loan fraud schemes and related Suspicious Activity Report filings. The Internal Revenue Service reports a significant increase in the number of fraudulent electronic tax returns that are based on bogus documents. Some fraudulent electronic tax returns have been used to obtain a refund anticipation loan. However, the limited number of Suspicious Activity Report forms reporting refund anticipation loan fraud indicates a possible lack of understanding of this crime and how financial institutions might be affected. To better assist financial institutions in identifying suspicious activity related to refund anticipation loan fraud, the following information is provided:

- A description of the legitimate process to obtain refund anticipation loans;
- A description of refund anticipation loan fraud schemes;
- Suspicious Activity Report filings and refund anticipation loan fraud case examples; and
- Examples of the types of transactions and activity, which may relate to refund anticipation loan fraud schemes.

Legitimate Refund Anticipation Loans

A refund anticipation loan is money borrowed by a taxpayer from a lender based on the taxpayer's anticipated income tax refund.[19] Other names for this type of loan are "Rapid Refund" and "Instant Money." The taxpayer signs a contract with a financial institution making the taxpayer responsible for repayment of the loan. Information on the tax return instructs the Internal Revenue Service to deposit the refund into an account in the name of the filer at the lending financial institution. The deposited money is then used to pay the loan balance. When the Internal Revenue Service

---

19 Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns, Pub. 1345, Rev. 1/2001

acknowledges acceptance of a tax return, they provide a debt indicator to inform the filer whether they have any outstanding debts that the refund will be used to offset. This information, along with other information gathered by the lender, is used to determine whether to extend the refund anticipation loan. There are numerous validity and consistency checks made by the Internal Revenue Service before an electronic return is accepted. One of those checks ensures the unique use of a valid Social Security number. The Employer Identification Number listed on the W-2 form also must be valid. However, the confirmation notice is not an agreement that the amount of the refund claimed on the tax return will be paid. The tax return must still pass through the Internal Revenue Service system, and the refund could be reduced or denied entirely. As of June 2000, the number of fraudulent electronically filed returns was one in 4,789; however, by the end of 2003, that number was one in every 966.[20]

How Refund Anticipation Loan Fraud Schemes Work

Fraud schemes involving income tax returns and refund anticipation loans typically entail creation of fake W-2 forms using the name and tax identifiers of real people and existing businesses. The perpetrator recruits individuals to pose as employees of a known business. These recruits could either be using their true identities or a stolen identity provided by the fraud perpetrator. When identity theft is involved, the recruit is given counterfeit identification documents, e.g., counterfeit Social Security cards and driver's licenses, to use as proof of identity. The recruited individuals find commercial tax preparers to file fraudulent electronic tax returns and then apply for a refund anticipation loan. The loan proceeds are then split between the fraud perpetrator and the recruit.

In another scheme, an unscrupulous electronic return originator will prepare a tax return for a taxpayer where only a small refund is claimed. The electronic return originator will pay the filer the refund in cash and the filer leaves. The electronic return originator will then manipulate the figures on the return and generate a much larger refund. The electronic return originator then requests a refund anticipation loan in the name of the taxpayer for the larger refund amount and files the tax return. The electronic return originator then negotiates the refund anticipation loan check and pockets the difference between what the true taxpayer was paid and the amount of the refund anticipation loan. This requires the electronic return originator to negotiate a large number of refund anticipation loan checks payable to other individuals. The large number of refund anticipation loan checks may be an indication of an electronic return originator abusing the refund anticipation loan process. The Federal statutory violations in these fraud schemes might include 18 U.S.C. §286, Conspiracy to defraud the United States by filing fraudulent income tax returns; 18 U.S.C. §287, Filing false claims against the United States; and 18 U.S.C. §1344, Bank Fraud.

---

20 Gary Bell, Director, Office of Refund Crimes, Internal Revenue Service Criminal Investigation, *Tax Fraud Alert: Fraudulent e-file Returns on the Rise*, http://www. Natptax.com/tax_news, last modified Feb. 23, 2004.

Suspicious Activity Report Filings

A search of FinCEN's SAR Query System revealed two Suspicious Activity Reports referencing refund anticipation loan fraud schemes.

- While conducting a routine review of its refund anticipation loans, a bank discovered similarities in multiple loan applications that indicated possible fraud. The bank found multiple W-2 forms that had unusually high withholding amounts (20 percent as opposed to the more typical 10 percent). Most of the suspicious loans included W-2 forms from well-known businesses. All of the W-2 forms had similar wages and withholding amounts. The tax returns on which the loans were based listed refundable credits (e.g., education credits, child care credits, and/or low income credits). Upon contacting the borrowers, the bank discovered that the income tax returns, which were the basis for these loans, were fraudulent. The names and Social Security numbers on the tax returns and loan applications had been obtained through identity theft. The employers listed on the W-2 forms did not employ the individuals named on the forms. The bank identified 41 fraudulent loans. The average refund on the fraudulent tax returns was $5,000.

- A bank filed a Suspicious Activity Report on loan fraud involving refund anticipation loans after the Internal Revenue Service failed to forward the refund checks for approximately 500 loans. The bank reported that it suspected the possibility of insider involvement on the part of the tax preparer because of a higher than normal charge for their service on the affected loans. (Note: After a subsequent law enforcement investigation and the issuance of Federal indictments, two subjects entered guilty pleas.)

No additional Suspicious Activity Reports describing fraudulent loans based on sham tax returns were located. However, there were nine reports of suspicious deposits of "Rapid Refund" or "Refund Anticipation Loan" checks. Each of these Suspicious Activity Reports related multiple deposits of this type of check into a customer's account. The checks were payable to individuals who endorsed them over to a third party. These Suspicious Activity Reports could be incidents of fraud perpetrators redeeming fraudulently obtained checks.

Refund Anticipation Loan Fraud Cases

The Internal Revenue Service named theft of personal and financial information used to file fraudulent tax returns as the second most common method of tax fraud. The combination of refund anticipation loan with a fraudulent tax return allows the perpetrator to take advantage of a source of funds that lenders advertise as instant money. To make this type of loan appealing to the public, funds are made immediately available, leaving little time for the lender to perform due diligence to prevent fraud. The following are examples of fraud schemes that used false income tax returns and refund anticipation loans.

- A February 2003 press release by the United States Attorney for the Southern District of New York announced the arrest of 17 defendants in connection with a tax and identity fraud scheme that allegedly netted more than $7 million.[21] The criminal Complaint charged the defendants with engaging in a scheme from 1997 through January 2003 to file thousands of false and fraudulent federal income tax returns. The defendants were accused of filing fraudulent returns for persons who were not entitled to the refunds. The defendants were also accused of committing identity theft to file tax returns on behalf of individuals without their knowledge. The fraudulent tax returns claimed Earned Income Credits and listed fake dependents. The tax returns were electronically filed and used to obtain refund anticipation loans.

- In 1998, a Federal court in the Western District of Tennessee convicted a man for bank fraud and filing false claims. The defendant was an accountant who prepared tax returns. The defendant created fictitious W-2 earnings statements using the names and Social Security numbers of low-income housing residents and individuals who were unemployed or receiving public assistance. He then electronically filed fraudulent tax returns and applied for rapid refund loans.

- Frequently, the tax preparer is an unwitting participant in these fraud schemes. In a court case filed in the United States District Court for Eastern District of Michigan, the defendant was convicted of conspiracy to defraud the government and submission of false claims to the government. The defendant prepared fake W-2 forms and caused a nationally known tax service provider to unwittingly electronically file the fraudulent tax returns. The defendant then received bank loans on the expected refund.

Refund Anticipation Loan Fraud Indicators

The IRS Restructuring and Reform Act of 1998 encouraged the Internal Revenue Service to set a goal of having 80 percent of Federal tax returns filed electronically by the year 2007. To aid in that goal, the Internal Revenue Service published a list of Free File Alliance tax preparers on its website who will electronically file income tax returns at no charge for persons who meet specified income criteria. An electronic return originator may submit either a tax return they have prepared or a return collected from a taxpayer. The Internal Revenue Service requests the electronic return originator be on the lookout for suspicious or altered income documentation (W-2 and 1099 forms), and requests (but does not require) that electronic refund originators obtain two forms of identification.[22] However, the electronic return originator who receives the return via the Internet is basically only transmitting the return to the Internal Revenue Service and does not have the opportunity to examine these documents.

---

21 For more information, see http://www.usdoj.gov/usao/nys/Press%20Releases/Feb03/IRSIDFRAUDARRESTS.pdf

22 *Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns*, Pub. 1345, Rev. 1/2001.

Extra precautions must be taken to prevent fraud associated with electronically filed income tax returns, especially when tax returns are submitted via the Internet. The Internal Revenue Service has a program that recognizes certain fraud indicators in electronically filed tax returns and prevents the issuance of some refunds based on the fraudulent returns. This program, however, will not protect the lending institution because the return is initially accepted and an electronic acknowledgement sent to the filer. It is the electronic acknowledgement that the lender uses to underwrite the loan. Electronic return originators/transmitters that accept income tax returns over the Internet also lack the advantage of personally meeting their customers.

Based on information from the review of Suspicious Activity Report narratives and criminal prosecutions, lending and financial institutions and tax preparers should be alert to the following "red flags" of possible refund anticipation loan fraud. Taken alone, these indicators may not involve activity related to refund anticipation loan fraud, but when they occur in combination, they should arouse suspicion.

1. Multiple loan applicants in a short time period with W-2 forms from the same employer;

2. W-2 forms that differ from other W-2 forms from the same employer or appear suspicious or altered;

3. W-2 forms with unusually high withholding amounts for the reported income – 20 percent as opposed to the more typical 10 percent;

4. Multiple W-2 forms that have identical, or nearly identical, income and withholding amounts;

5. Tax returns that include tax credits (i.e., Earned Income Credit, education credits, child credits);

6. Customers whose identification addresses do not match the address on the W-2 forms;

7. Customers using "mail drop" addresses, e.g., United States Post Office boxes, retail postal services addresses, etc.;

8. Multiple refunds directed to the same address or post office box;

9. Loan applicants presenting identification documents that appear counterfeit;

10. Multiple direct deposits from tax refunds deposited into the same account; or

11. Individuals depositing (or cashing) multiple refund anticipation loan checks payable to third parties.

Finally, an Internal Revenue Service refund that is intended to satisfy an outstanding refund anticipation loan balance but that is not received within the typical time frame (about two weeks) could indicate the Internal Revenue Service has identified the refund as possibly fraudulent.

What to do if Suspicious Activity is Suspected

In accordance with Suspicious Activity Report regulations, financial institutions are required to report suspicious activity, including those that involve a refund anticipation loan, whenever they suspect their institution was used to facilitate criminal transactions when the amount aggregates to the applicable suspicious activity reporting thresholds. When completing a Suspicious Activity Report form to report activity indicative of refund anticipation loan fraud, a depository institution preparer should mark box 35g, Consumer Loan Fraud, and use the narrative to clearly, completely and sufficiently explain the nature of the refund anticipation loan fraud. Other types of financial institutions that know or suspect that transactions may involve proceeds from refund anticipation loan fraud should mark the "Other" box and provide an explanation in the narrative that completely and sufficiently explains why the institution suspects or has reason to suspect the transactions.

Broker-Dealer Suspicious Activity Reports – The First Year

The broker-dealer suspicious activity reporting requirement became effective January 1, 2003 for broker-dealers not affiliated with banks or bank holding companies. To provide feedback to the broker-dealer community as part of its ongoing efforts to enhance suspicious activity reporting quality, FinCEN undertook a two-pronged feedback project. First, FinCEN surveyed law enforcement agencies to determine how broker-dealer Suspicious Activity Reports are being used, whether they add value to cases, and where improvement is needed. Second, FinCEN reviewed its own proactive targeting efforts to determine how broker-dealer Suspicious Activity Reports have helped to develop leads for law enforcement. The results of the feedback project are described below.[23]

Law Enforcement Feedback

FinCEN asked federal law enforcement users whether they regularly review broker-dealer Suspicious Activity Reports, how they use broker-dealer Suspicious Activity Reports, whether any cases have been initiated in which a broker-dealer Suspicious Activity Report contributed useful information, and whether there are any areas where Suspicious Activity Report quality could be improved.

---

23 For specific statistical data related to SAR filings by broker-dealers, refer to Section 4 of Issue 2 of *The SAR Activity Review – By the Numbers*, found on the FinCEN website, www.fincen.gov under Regulatory/SAR Information.

At the time of the survey, not all law enforcement agencies regularly reviewed all broker-dealer Suspicious Activity Report filings, although one of the results of this survey was to stimulate interest in implementing a regular review process. Those investigators that regularly review broker-dealer Suspicious Activity Reports do so in a number of ways, including retrieval by type of violation the agency is interested in, and sampling for trends and investigative analysis. Some multi-agency groups reported reviewing all Suspicious Activity Reports filed for their geographic district. The most frequent use of broker-dealer Suspicious Activity Reports this past year was to add value to ongoing cases. For example, one agent found a broker-dealer Suspicious Activity Report helpful in clarifying events and dates in an ongoing investigation; this led him to conduct interviews that would not have been considered important and may have been overlooked prior to reviewing the Suspicious Activity Report. Another interesting example of the value of broker-dealer Suspicious Activity Reports to ongoing investigations is their use in tracing illicit proceeds, as described below.

Case #1: In a fraud/money laundering investigation, investigators found a Suspicious Activity Report filed by a broker-dealer on the target of the investigation that described the quick movement of money in and out of a brokerage account. The identifiers on the Suspicious Activity Report were used to search the database, generating other Suspicious Activity Reports, a Currency Transaction Report and a Report of Foreign Bank and Financial Accounts. This trail led to the discovery of a bank account in another country into which the illicit proceeds had been deposited. The investigation is ongoing.

Case #2: A broker-dealer Suspicious Activity Report contributed to the jailing of a fraud defendant subject to an order requiring the payment of millions of dollars to the government. Investigators found a broker-dealer Suspicious Activity Report filed on the defendant describing activity inconsistent with the nature of the account. They followed the money trail from the Suspicious Activity Report to a bank where the defendant purchased money orders. The money orders, in turn, were used to purchase postal money orders, which were then deposited into a bank account in the United States. The defendant then transferred these funds to an offshore account. The defendant, who had concealed, transferred, and lied about his assets, was found in contempt of court and jailed. The funds are in the process of being repatriated.

Case #3: Suspicious Activity Reports filed by a depository institution and broker-dealers led to the successful prosecution of a union official who had misappropriated union funds. Discrepancies in several of the union's accounts resulted in the filing of a Suspicious Activity Report that initiated an investigation by the Federal Bureau of Investigation, which uncovered evidence of a multi-million dollar embezzlement. A subsequent search through Gateway[24] revealed two broker-dealer Suspicious

24 FinCEN's Gateway Program enables federal, state and local law enforcement agencies to have direct, on-line access to records filed under the Bank Secrecy Act.

Activity Reports showing suspicious wire transfer activity. According to the case agent, the broker-dealer Suspicious Activity Reports saved a great deal of time in "following the money." The agent handling the case commented that, without the assistance of the Suspicious Activity Reports, he never would have thought to look for the money in the direction where the reports indicated. Several subpoenas were issued as a result of the broker-dealer Suspicious Activity Reports, which led to valuable information. To date, this case has resulted in the filing of charges against three defendants, one conviction, and millions in court-ordered forfeiture.

Case #4: A broker-dealer Suspicious Activity Report aided in an investigation conducted jointly by the Federal Bureau of Investigation and Internal Revenue Service Criminal Investigation of an embezzlement scheme perpetrated by an accountant for a construction company who had "disappeared." The investigation determined that before his disappearance, he had systematically embezzled funds from the company. The Federal Bureau of Investigation, with the assistance of agents with the Bureau of Customs and Border Protection (legacy United States Border Patrol), arrested the accountant. The subject agreed to cooperate and plead guilty to a superceding bill of information charging the original bank fraud charges as well as tax fraud and conspiracy to violate tax laws. Subsequent investigation discovered millions of dollars of unreported income as well as the involvement of other individuals in the criminal activities. Additional charges are anticipated. The information from the broker-dealer Suspicious Activity Report helped identify assets and sources of income. Substantial documents and account records identified and obtained as a result of the Suspicious Activity Report aided in identifying funds generated by the scheme. The investigating agent found the Suspicious Activity Report to be robust and detailed, containing much pertinent and valuable information necessary for effective follow-up.

Suspicious Activity Report Quality

In general, federal law enforcement investigators reported they were satisfied with the quality of the broker-dealer Suspicious Activity Reports they reviewed during calendar year 2003. The most frequently identified area for financial institutions' improvement was Suspicious Activity Report completeness. More specifically, when asset movement is reported, Suspicious Activity Reports sometimes do not include identifiers for the transferee, such as, where applicable, name and location of the receiving financial institution, and account name and number of the beneficiary. Having this information articulated in the Suspicious Activity Report can save valuable time and steps in an investigation, especially when assets are in motion. This information should be placed in the Suspicious Activity Report narrative section.

Proactive Targeting

FinCEN's Proactive Targeting Unit has developed a number of cases through review, analysis, and data mining of broker-dealer Suspicious Activity Reports. Once

developed, such cases are referred to the appropriate law enforcement agency. Two illustrative cases are described below.

The first case developed from broker-dealer Suspicious Activity Reports disclosing what appeared to be an ongoing fraud scheme by a group of individuals and entities purporting to operate a hedge fund. According to the Suspicious Activity Report narrative, the address given for the hedge fund turned out to be a post office outlet and the telephone number belonged to an answering service. Funds received in the account were the subject of numerous unexplained wire transfers to foreign countries. Research by FinCEN disclosed Currency Transaction Reports filed by financial institutions on the hedge fund showing large cash transfers made by the hedge fund to an individual. That individual, in turn, was the subject of Currency Transaction Report forms reporting that he moved $12 million in cash transactions through two different companies, both with the same Employer Identification Number and bank account. That same individual was the subject of numerous Currency Transaction Report by Casino filings during the same period. The individual, and the individual and corporate subjects of the Suspicious Activity Reports, were also named in several different criminal investigations.

FinCEN developed another proactive case as the result of analysis of two Suspicious Activity Reports that reported possible money laundering and wire transfers without economic purpose in brokerage accounts through which money moved between foreign pawnshops and the United States. The brokerage accounts had numerous third-party wires with minimal brokerage activity. There were also a limited number of large-dollar check transactions among the subjects involved in these transactions. FinCEN research discovered two Currency Transaction Report filings on a person with the same last name and foreign address as one of the subjects, who gave two different occupations to the two different bank filers. Commercial database research provided additional links among the various subjects.

FinCEN intends to continue monitoring the various categories of Suspicious Activity Reports, especially the new categories of filers, to provide ongoing feedback. In the next issue of *The SAR Activity Review*, we intend to focus on Suspicious Activity Reports filed by casinos, an industry with mandated Federal Suspicious Activity Report filing requirements effective March 2003.

Automated Teller Machine - Commonly Filed Violations

Automated teller machines have become an ubiquitous part of our everyday lives. The number of automated teller machines has grown exponentially since 1969 when the first machine was put into service. Today, in the United States alone, there are an estimated 388,500 automated teller machines. These customer-friendly portals provide a wide array of banking services, are available 24 hours a day, and are found in almost every imaginable location. The wide availability and ease of use of auto-

mated teller machines allow people to conduct financial transactions with greater flexibility and convenience. Unfortunately, criminals also use automated teller machines. Money launderers, in particular, have found automated teller machines to be a convenient and relatively less risky way to structure transactions to avoid the various reporting requirements of the Bank Secrecy Act. Check fraudsters have also found that passing insufficiently funded checks through an automated teller machine provides them with a greater degree of anonymity.

As a follow-up to previous *SAR Activity Review* articles and to *SAR Bulletin - Issue 1* (June 1999), FinCEN sampled Suspicious Activity Reports filed after *SAR Bulletin – Issue 1* was published to determine if identifiable patterns of suspicious activity associated with automated teller machines had changed appreciably. This analysis showed that the two prominent suspicious activities identified in 1999, use of automated teller machines as a way of avoiding certain Bank Secrecy Act requirements and check fraud, still represent the primary trends of suspicious activities reported in current Suspicious Activity Report filings.

Continued Use of Automated Teller Machines to Avoid Bank Secrecy Act Reporting Requirements

As was previously noted in *SAR Bulletin – Issue 1*, automated teller machines continue to be used by some to avoid the Currency Transaction Report. It is also suspected that money launderers and other criminals are using automated teller machines to avoid filing Reports of International Transportation of Currency and Monetary Instruments.

Cross Border Currency Movements

Law enforcement investigations reveal that drug dealers frequently use domestic automated teller machines to deposit illicit proceeds into financial institution accounts and then withdraw the funds from automated teller machines located in their drug suppliers' countries of origin. This method is a way to avoid the risks associated with bulk cash smuggling and the enhanced scrutiny of law enforcement at the borders. This technique also facilitates avoidance of a Report of International Transportation of Currency and Monetary Instruments filing. This same method can be used to move virtually any other type of illicit proceeds.

A recent analysis by FinCEN found that financial institutions located in Florida file the majority of Suspicious Activity Reports that report suspicious cash withdrawals from automated teller machines in foreign countries. This finding likely is due to Florida's close proximity to the Caribbean and Latin America as well as Miami's role as an international travel hub. Florida also has a renowned tourism industry and, consequently, a strong cash economy. Money launderers prefer to operate in cash intensive areas like south Florida hoping that the likelihood of "illegal" cash being detected will be significantly reduced.

In addition, Suspicious Activity Reports sampled in FinCEN's analysis identified various monetary instruments deposited into accounts, with funds withdrawn shortly thereafter from foreign automated teller machines. In some instances, cash combined with other monetary instruments were deposited during a single transaction. Some of those other monetary instruments included:

- personal checks;
- cashiers checks;
- international money orders;
- other money orders; and
- funds from redeemed Certificates of Deposit.

Suspicious Activity Report filings reported that these types of deposits were followed quickly by daily maximum cash withdrawals through automated teller machines located in foreign countries. The majority of withdrawals cited were from automated teller machines located in Colombia. The size and number of the cash withdrawals within short time frames indicate possible money laundering.

Currency Reporting Requirement

FinCEN's recent analysis also found continued prominent reporting of automated teller machines being used to structure currency transactions in order to avoid the Currency Transaction Report filing requirements. Suspicious Activity Reports indicated two prevalent patterns of structuring: customers making multiple cash deposits and/or withdrawals aggregating to sums over $10,000 on the same day at one or more automated teller machine locations, and customers using a combination of same-day teller and automated teller machine activity. Some examples of this type of activity are:

- **Automated teller machines only**[25]
    - Four individuals deposit/withdraw $3,000 on the same day at seven different automated teller machines.[26]

25 The automated teller machine activity could apply to transactions occurring either for an account owned by one or more customers or among multiple accounts owned by one or more customers.

26 Most domestic financial institutions and host networks limit daily automated teller machine withdrawal amounts to between $300 and $500. However, each institution and host network, taking into consideration risk management and client relationship concerns, determines its own automated teller machine limits.

- One individual deposits/withdraws $3,000, several different times during the day, using the same automated teller machine.

- **Automated teller machine in combination with other types of transactions**

  - An individual cashes a check with a teller in a financial institution for $9000 followed by three $500 automated teller machine withdrawals.

  - An individual deposits $8000 in cash with a teller in a financial institution followed by several $1,000 cash deposits through an automated teller machine.

In several instances, the filing financial institutions reported that the structured cash deposits consisted of all $100 bills or $20 bills. For example, it is not uncommon for drug dealers to use $100 bills for bulk payments since it allows the cash to be concealed in smaller containers such as a brief case for easier and less detectable transport. Conversely, smaller denominations, such as $20 bills, are considered by law enforcement as "street money" for purchasing drugs. Large deposits consisting of $20 bills at an automated teller machine also could represent funds withdrawn from another automated teller machine, with the successive transactions being an attempt to layer the movement of funds.

Check Fraud Violations

The majority of Suspicious Activity Reports citing check fraud violations in connection with automated teller machine usage involved insufficiently funded or "worthless"[27] checks deposited in automated teller machines. Many of the Suspicious Activity Reports sampled for this study reported that before these deposited checks were returned unpaid, the accounts were depleted through checks, point of sale debits, or cash withdrawals at automated teller machines, often resulting in a net loss to the bank.[28] This type of activity can be spread across multiple accounts and involve multiple financial institutions. For example, one financial institution linked 15 accounts to a fraud ring that engaged in worthless check deposits while another financial institution linked the same activity to approximately 175 other accounts.

What to do When Suspicious Activity is Suspected

When reporting suspicious activity involving automated teller machines, financial institutions are encouraged to file complete and sufficient Suspicious Activity Reports

27 "Worthless" is a term used in the Suspicious Activity Report narratives to describe, among other things, checks that are drawn on insufficient funds or closed accounts; stolen, forged or counterfeit checks (identity theft); or checks on which payment has been stopped.

28 The total loss amount related to check fraud conducted through automated teller machines is not readily available since some Suspicious Activity Report filers do not include a loss amount.

and are reminded to include the dollar amount involved; for depository institution filers, if applicable, include the amount of loss prior to recovery (Item #36 on the Suspicious Activity Report form) and the dollar amount of recovery (Item #37).

Conclusion

Bank Secrecy Act/Structuring/Money Laundering and Check Fraud continue to be the two most frequently reported characterizations of suspicious automated teller machine activity cited in Suspicious Activity Report narratives. Although it appears that automated teller machines are still being used for various forms of structuring and check fraud, it also appears that many financial institutions faced with this activity are using their Bank Secrecy Act compliance programs to detect and report it in a timely manner.

FinCEN is in the process of learning more about the operations associated with the automated teller machine industry, including the role of Independent Sales Organizations and sub-Independent Sales Organizations that own and operate automated teller machines in the United States. FinCEN intends to work with the automated teller machine industry, law enforcement and the regulatory community to study the vulnerabilities associated with Independent Sales Organizations and sub-Independent Sales Organizations in their operations.

Consumer Loan Fraud

FinCEN recently conducted an analysis of Suspicious Activity Reports citing incidents of consumer loan fraud to identify trends and patterns associated with this crime. The study encompassed Suspicious Activity Reports filed between April 1996 and September 30, 2003. A significant finding of this study was that the total number of Suspicious Activity Reports filed by financial institutions between 1997 and 2002 reporting consumer loan fraud increased 54%.

The narratives of a sample of 2,126 Suspicious Activity Reports filed between January 1, 2001 and September 30, 2003 were reviewed to determine changes in fraud by type of loan. The findings revealed filings on personal unsecured loans increased by 78%; filings on home equity loans increased by 56%; filings on secured loans increased by 41%, and filings on student loan fraud increased by 10%. However, incidents of reported automobile loan fraud decreased by 35%.[29]

The study identified three major trends in consumer loan fraud: a steady increase in the use of remote loan applications over the Internet and telephones to commit

29 Credit Card loans were classified as "unclassified loans" in this study. Please note that the 2003 Suspicious Activity Reports were for a 9-month period between January 1st and September 30th.

fraud; a marked increase in the incidents of credit bust-out schemes;[30] and a significant increase in fraud involving income tax refunds and refund anticipation loans.

FinCEN will soon publish an Advisory on consumer loan fraud to report the complete findings of the study. The report will include suggestions for enhancing due diligence efforts and risk management programs. This Advisory will be available on the FinCEN website, www.fincen.gov. Until that report is published, to learn more about refund anticipation loan fraud schemes, see the analysis of refund anticipation loan fraud appearing elsewhere in this section.

30 In a credit bust-out scheme, a suspect obtains a credit card or line of credit, charges or uses up to the maximum credit limit and then pays off the outstanding debt with a worthless check. This results in immediate credit extended again up to the maximum limit. The cycle is immediately repeated. By the time the bad check is returned, the debt is double the credit limit. This activity may continue for two or three billing cycles before the lender freezes the account and begins the collection process.

Section 2 – Law Enforcement Cases

This section of *The SAR Activity Review* affords law enforcement agencies the opportunity to summarize investigative activity in which Suspicious Activity Reports and other Bank Secrecy Act information played an important role in a successful investigation and prosecution of criminal activity. Each issue includes new examples based on information received from federal, state and local law enforcement agencies. Other law enforcement cases can be found on the FinCEN website, www.fincen.gov in the Law Enforcement / LEA Cases Supported by BSA Filings section. This site is updated periodically to include new cases of interest.

Update on the USA PATRIOT Act Section 314(a) System

In the November 2003 issue of *The SAR Activity Review – Trends, Tips & Issues*, FinCEN provided information about the results of the 314(a)[31] requests sent to financial institutions from February through October 20, 2003. This section will update that process and includes 314(a) requests sent through June 30, 2004.

FinCEN submitted 285 Section 314(a) requests on behalf of 11 individual Federal law enforcement agencies to 33,735 financial institutions between February 18, 2003 and June 30, 2004. The agencies only submitted 314(a) requests in the conduct of the following significant criminal investigations – Terrorism (103) and Money Laundering (182).

The 285 cases submitted included 1,988 subjects of interest. Through June 30, 2004, 14,135 positive responses were received from financial institutions, which were forwarded to law enforcement requesters by FinCEN. Of the 14,934 total responses received from financial institutions, 799 were inconclusive.

Law enforcement requesters were asked to provide information about the utilization of the financial information received for the 314(a) requests sent from February 2003 through June 2004. The requesters responded with the following results as of June 30, 2004:

- 1,236 new accounts located;
- 73 new transactions identified;

31 Under Section 314(a) of the USA PATRIOT Act, FinCEN issued a rule, which established a system to enable law enforcement officials, who are investigating terrorist financing cases or major money-laundering cases, to relay targets of investigations to financial institutions for real time responses.

- 601 Grand Jury subpoenas served;
- 11 Search Warrants executed;
- 129 Administrative Subpoenas/Summons issued;
- 9 individuals arrested; and
- 2 individuals indicted.

Investigations Assisted by Suspicious Activity Reports

314(a) Results Greatly Enhance Case Involving Material Support to Terrorism

A multi-agency task force, led by the Bureau of Immigration and Customs Enforcement and including the Federal Bureau of Investigation and Internal Revenue Service Criminal Investigation, is investigating violations related to money laundering, tax fraud and material support to terrorism. As a result of this investigation, 33 search warrants have been executed and over 400 Grand Jury subpoenas for bank account and brokerage accounts have been issued. To date, two suspects have been arrested; one has been convicted of immigration violations and the other suspect has been indicted for violations of immigration laws and the International Emergency Economic Powers Act. This investigation has been greatly enhanced by the results of a 314(a) request, which identified over 200 bank and other financial institution accounts affiliated with the targets of the investigation. (*Source: Bureau of Immigration and Customs Enforcement)*

Individual Sentenced for Operating an Unlicensed Money Transmitting Business & Bankruptcy Fraud

An individual was recently sentenced in United States District Court to six months in prison for operating an unlicensed money transmitter business and for bankruptcy fraud. The subject was also ordered to forfeit over $25,000. This case was initiated after the review of numerous Suspicious Activity Reports filed by several banks that reported the target was making cash deposits inconsistent with the individual's occupation as a minimum wage employee. Various investigative techniques, including the analysis of Currency Transaction Report and Suspicious Activity Report filings and the execution of several search warrants, ultimately led to the target's conviction.

According to court records filed, the target made numerous cash and check deposits to several accounts and subsequently wired these funds to several foreign countries in Asia, Europe, South America, and the Middle East. During a 4½-year period, the target wired over $3 million out of the country.

Agencies participating in this investigation include the Internal Revenue Service Criminal Investigation and the Federal Bureau of Investigation. *(Source: Internal Revenue Service Criminal Investigation)*

Suspicious Activity Reports Identify Non-Profit Organizations as Illegal Money Remitters

In 2003, Bureau of Immigration and Customs Enforcement agents initiated an investigation of several non-profit organizations in the United States. These were all registered as tax-exempt organizations. The investigation revealed the organizations were operating as illegal wire remitting businesses, allegedly co-mingling drug proceeds with donations. Suspicious Activity Report documentation revealed approximately $3 million in transactions during a three-month period.

Examination of Suspicious Activity Reports determined that most incoming funds were from "donations" and a large number of third party deposits. Funds were transferred out of the account using checks, cashier's checks and wire transfers to a number of entities. Outgoing funds were often sent to accounts affiliated with suspected criminal organizations. *(Source: Bureau of Immigration and Customs Enforcement)*

Bank Secrecy Act Data Leads to Seizure of $18 Million

Agents with the Bureau of Alcohol, Tobacco, Firearms and Explosives conducted an investigation into the illegal sale of cigarettes that led to the indictment of 13 defendants. Cigarettes that were purchased in a low tax state were sold in a high tax state without the payment of taxes in either location. Auditors and analysts utilized Bank Secrecy Act data to identify bank accounts that were used by the defendants to hide and transfer illicit gains from the cigarette sales. Some funds were laundered through the purchase of property, including homes and vehicles, and other funds were transferred overseas. It appears that the parties involved are part of a larger Russian organized crime operation. Other Bank Secrecy Act data was useful in identifying assets totaling over $18 million, which were seized by the United States Government. *(Source: Bureau of Alcohol, Tobacco, Firearms and Explosives)*

Suspicious Activity Reports Aid in Ponzi Scheme Investigation

A subject was sentenced in United States District Court to serve the longest prison term possible under Federal sentencing guidelines for claiming he was earning huge profits on a stock trading formula where he was actually using investors' money to buy homes and luxury items. The subject was also ordered to pay several million dollars in restitution to the victims of his Ponzi scheme. (In a Ponzi scheme, the perpetrator uses funds from new investors to pay earlier investors.)

The evidence presented at trial proved the subject obtained millions from several hundred investors through this scheme. Instead of investing his victims' money, the

subject spent it on himself and his wife, on purchases of luxury items, homes, vehicles and a yacht, and to finance a web site.

The victims in this investigation included stockbrokers, investment advisers, lawyers, court reporters, engineers, airline pilots, doctors, and real estate brokers. A number of the victims retired from their jobs because they believed they were rich after having invested their retirement savings with the subject. The scheme collapsed when the subject ran out of money and suspicious investors called the Federal Bureau of Investigation.

According to agents, Bank Secrecy Act reports greatly assisted the investigation. Searches resulted in identifying several Suspicious Activity Reports totaling almost $1.2 million, several Currency Transaction Reports totaling over $42,000, and numerous Currency Transaction Report by Casinos filings, which totaled almost $650,000. These reports helped to document the pattern of the money flow. *(Source: Federal Bureau of Investigation)*

Suspicious Activity Reports Identify Money Laundering Activities

In December 2002, the New York office of the Bureau of Immigration and Customs Enforcement's El Dorado Task Force identified numerous Suspicious Activity Reports that showed a pattern of suspicious financial transactions conducted by a company in the New York area. The company was identified as a money exchange business located in South America with several bank accounts in New York. The investigation revealed several companies and individuals utilizing the black market peso exchange to launder alien smuggling proceeds in violation of Title 18 U.S.C. 1956, Money Laundering.

Specifically, the agents identified five co-conspirators allegedly involved in structuring deposits of cash, using third-party and payroll check deposits into at least two bank accounts. Subsequently, the funds were remitted to other companies and individuals located in the southeast and southwest.

In the fall of 2003, Bureau of Immigration and Customs Enforcement agents arrested the main target for violations of 18 U.S.C. 1960, Unlicensed Money Service Business and 18 U.S.C. 1956, Money Laundering. The investigation and Suspicious Activity Reports showed the target structured $500,000 in third-party and payroll checks into two of his personal accounts, and subsequently wire transferred the funds to other areas in the United States. *(Source: Bureau of Immigration and Customs Enforcement)*

Suspicious Activity Reports Useful in Round-Tripping Investigation

The United States Secret Service, New York Field Office, seized over $5.3 million from a correspondent account for a bank headquartered in Nigeria. Investigative leads derived from Bank Secrecy Act data determined that this account was actually

owned by the Nigerian bank and operated by the bank's president and chairman of the board of directors. Information obtained from a review of Bank Secrecy Act filings determined that this bank was operating a highly sophisticated hedging scheme called "round-tripping[32]." The elaborate scheme involved offshore bank accounts and included the use of International Business Corporations. The information obtained from Bank Secrecy Act data, including Suspicious Activity Reports, financial reports, travel records, and suspect information, among others, led to the Default Judgment in favor of the Government in 2003, issued by a United States District Court.

This case resulted in the May 2002 suspension of over 21 Nigerian banks by the Federal Republic of Nigeria's Economic and Financial Crimes Commission.[33] This case also led to the arrest of Nigeria's Director of Immigration, the first Nigerian Government Official ever arrested for "419" Fraud.[34] As a result, the Nigerian government established a new Office of Economic Recovery to combat the round-tripping epidemic in that country. *(Source: United States Secret Service)*

Suspicious Activity Reports Assist Telemarketing Fraud Investigation

Two partners were sentenced to prison as a result of their involvement in a telemarketing fraud. According to the United States Attorney's Office, the partners owned a telemarketing business and admitted that employees of that business used pre-text calling to obtain information from numerous companies across the United States. The telemarketing company would use that information in a second telephone call to the business owner and fraudulently tell them they were affiliated with the business owner's regular supplier and that they could buy supplies from the telemarketing company for a reduced price.

However, the investigation documented that the price charged was two to three times higher than the actual retail value of the supplies; incomplete orders were shipped but billed as complete orders; and, furthermore, the supplies that the defendants shipped were defective. In total, the partners bilked numerous companies, including large, multi-national corporations. In addition, the investigation determined that the total amount of the fraud was more than $3 million. The subject also admitted that his partner conspired to evade corporate income taxes of their telemarketing company by having approximately $3 million in corporate checks made out in the name of others, and that the subject failed to report almost

32 Press releases related to enforcement actions from the United States Securities and Exchange Commission describe "round-tripping" as a scheme in which funds are circulated from an entity through companies purporting to be customers and vendors of that entity in what were actually fictitious transactions. It is accomplished by simultaneous, pre-arranged buy-sell trades with the same counter-party, at the same price and volume, and over the same term, resulting in neither profit nor loss to either transacting party.

33 Nigeria's Economic and Financial Crimes Commission is responsible for enforcing and administering Nigerian laws related to money laundering, advance fee schemes, fraud and other financial crimes within the country.

34 "419" refers to the section in the Nigerian penal code that deals with advance fee fraud. For more information about this crime, refer to Issue 3 of *The SAR Activity Review – Trends, Tips & Issues*, page 23, published in October 2001 at http://www.fincen.gov/sarreviewissue3.pdf.

$300,000 in income to the Internal Revenue Service on one year's federal tax return. These and other actions by the subject's partner resulted in unpaid federal income taxes of approximately $750,000. This investigation was initiated after the review of numerous Suspicious Activity Reports filed by financial institutions. *(Source: Internal Revenue Service Criminal Investigation)*

Ex-Bank President Guilty in Loan Fraud After Investigation Initiated by Suspicious Activity Report Filing

Through the review of a Suspicious Activity Report, the Federal Bureau of Investigation launched an investigation into an internal bank fraud that resulted in the conviction of the former president of the bank and his personal banking customer. In 2003, the two defendants were convicted at trial for their roles in a nominee loan fraud committed against the bank. The two had been accused of hiding the purpose behind a significant increase in a line of credit from the bank to the customer. The banker reportedly helped his customer increase his credit limit at the bank, but all of the extra money went back to the banker for a real estate investment. As a part of the fraud, the banker signed a loan document stating that credit was not being extended to anyone other than the customer, when in fact the banker was the beneficiary of the loan. Additionally, the banker was convicted on a count alleging he signed a personal financial statement that concealed the fact that he had borrowed money from the customer.

The banker and his customer were sentenced in early 2004 to lengthy prison terms. In addition, the Federal Bureau of Investigation was successful in having $ 1.5 million in assets forfeited to the United States Government. *(Source: Federal Bureau of Investigation)*

Suspicious Activity Report Leads to Forfeiture of Currency

A Suspicious Activity Report filing prompted a Bureau of Immigration and Customs Enforcement investigation into the activities of a subject from another country. The Suspicious Activity Report alleged that after an initial account opening deposit, the subject had structured deposits exceeding $700,000. Investigation revealed this suspect was known as a mid-level narcotics trafficker in his home country. In collaboration with the Federal Bureau of Investigation, the currency was seized from the bank account and the case filed for civil forfeiture in State District Court. In a recent out of court settlement, the suspect agreed to forfeit fifty percent of the monies. *(Source: Bureau of Immigration and Customs Enforcement)*

State and Local Law Enforcement's Use of Suspicious Activity Report Data

The following cases obtained through the FinCEN Gateway Program demonstrate state and local governments' use of Suspicious Activity Report data.

Bank Secrecy Act Reports Instrumental in Investigation and Conviction of Attorney and Three Accomplices in Multi-Million Dollar Real Estate Fraud

In 2003, four individuals, previously convicted of charges related to a multi-million dollar real estate scheme, were ordered to pay over $1 million in restitution to reimburse victims of their crimes. According to court documents, a real estate investor and an attorney arranged for the proceeds of fraudulent real estate transactions to be deposited into the attorney's trust account. The attorney subsequently withdrew funds from this trust account for personal use and the use of the co-conspirators.

This complex real estate fraud investigation was enhanced through the state law enforcement agency's pro-active review using FinCEN's Gateway Program to search the Currency and Banking Retrieval System database for Bank Secrecy Act reports relating to the four subjects. This search identified 100 Currency Transaction Reports, 11 Currency Transaction Reports by Casinos, 2 Reports of International Transportation of Currency or Monetary Instruments, and 5 Suspicious Activity Reports. According to the investigator, this pro-active review resulted in the initiation of the investigation. The search also identified reports of additional transactions conducted at a local check cashing company. One of the Suspicious Activity Reports provided information that one subject was cashing checks at the check cashing company for an attorney. The investigator found all of the Bank Secrecy Act documents very useful in this investigation.

Suspicious Activity Reports Aid Conviction of Drug Dealers

In 2003, two defendants plead guilty to multiple drug-related and money laundering charges. A third subject pled guilty to an additional charge of Dealing in Unlawful Proceeds.

Narcotics agents with a State Attorney General's Office initiated the investigation as an interdiction case. The agents stopped one subject at a bus station in a city, en route between two other large, metropolitan cities. This subject told agents he was to meet two men in a vehicle parked near the bus station that same day to sell the drug Ecstasy for approximately $100,000. State agents and city police narcotics detectives set up surveillance and observed two men sitting in a vehicle parked at the location described by the first subject. These men were detained, a search warrant was obtained, and a large sum of cash was found in the vehicle. The men

told agents they were going to use the money to buy the Ecstasy pills. Those men were arrested and charged.

The agents used FinCEN's Gateway Program to conduct a review of the Currency and Banking Retrieval System database for Bank Secrecy Act reports relating to the three subjects. The search located six Currency Transaction Reports and one Suspicious Activity Report. The case agent said the Suspicious Activity Report information, coupled with statements at the time of arrests, ultimately led to the money laundering convictions, as well as identified bank accounts. The agent executed a search warrant at one financial institution and obtained bank documents that enabled him to construct a net worth analysis. The second count of money laundering was based on information from files at an automobile dealership where another search warrant was executed. That file contained an Internal Revenue Service Form 8300 (Report of Cash Payments over $10,000 Received in a Trade or Business) showing one of the subjects paid cash for the vehicle he used to pick up the Ecstasy pills.

Suspicious Activity Reports Assist in Investigation of Insurance Executive for Embezzling from Local Government's Self-Insured Health Care Fund

In 2003, an insurance executive pled no contest and was found guilty on a single count of aggravated theft. The defendant admitted misappropriating money that was intended to pay medical claims for the local government's self-insured health benefits plan. Acting as the health insurance agent for the local government, the executive failed to fully credit the government's account for payment of the health insurance premiums after receiving two large checks.

The state law enforcement agency initiated this investigation and provided their findings to the State's Department of Insurance. Research was conducted using FinCEN's Gateway program to access the Currency and Banking Retrieval database for Bank Secrecy Act reports relating to the insurance executive. An analyst reported that Suspicious Activity Report documentation was beneficial to the investigation since it identified two accounts held at two banks and reported check kiting from the subject's business account to a personal account.

The executive received a prison sentence, agreed to a permanent revocation of his license to sell insurance in the State and repaid most of the funds embezzled from the local government.

Section 3 - Tips on Suspicious Activity Report Preparation & Filing

Suspicious Activity Reporting Guidance Package

In November 2003, FinCEN, in consultation with the federal regulatory authorities, issued a guidance package designed to assist financial institutions in preparing Suspicious Activity Report forms and improving the quality of information provided in Suspicious Activity Report narratives. The guidance package consists of three parts:

Part I: *Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative;*

Part II: *The Suspicious Activity Report (SAR) Form* (a PowerPoint presentation); and

Part III: *Keys to Writing a Complete & Sufficient SAR Narrative* (also a PowerPoint presentation.)

This guidance package is found on the FinCEN website at http://www.fincen.gov/narrativeguidance_webintro.pdf. Financial institution Bank Secrecy Act compliance officers, law enforcement officials and others may download the PowerPoint presentations to complement their existing Bank Secrecy Act and anti-money laundering training programs.

Suspicious Activity Reporting Guidance for Casinos

In December 2003, FinCEN also released a guidance package specifically designed to provide assistance to casinos. This publication, *Suspicious Activity Reporting Guidance for Casinos*, which should be used as a supplement to the Suspicious Activity Report by Casino form instructions, is found at http://www.fincen.gov/casinosarguidancefinal1203.pdf.

How do I . . . ?

In addition to the publication of the guidance packages in the Fall 2003, every previous issue of *The SAR Activity Review* includes tips on how to properly prepare Suspicious Activity Report forms. Following is a listing of some of those past topics.

Topic	Issue	Page	Hyperlink Address
Reporting Computer Intrusion and Frequently Asked Questions	3	38	http://www.fincen.gov/sarreviewissue3.pdf
Filing a Corrected or Amended Suspicious Activity Report	4	42	http://www.fincen.gov/sarreview082002.pdf
Filing a Suspicious Activity Report for Ongoing or Supplemental Information	4	43	http://www.fincen.gov/sarreview082002.pdf
Reporting Identity Theft and Pretext Calling	3	41	http://www.fincen.gov/sarreviewissue3.pdf
Importance of Accurate and Complete Narratives	5	55	http://www.fincen.gov/sarreviewissue5.pdf
Improvements to Eliminate Reporting Deficiencies	6	49	http://www.fincen.gov/sarreviewissue6.pdf
Informal Value Transfer System—Special Suspicious Activity Report Form Completion Guidance	5	57	http://www.fincen.gov/sarreviewissue5.pdf
Instructions for Completing the Suspicious Activity Report Form	6	50	http://www.fincen.gov/sarreviewissue6.pdf
Suspicious Activity Report Filing Tips for Money Services Businesses	4	42	http://www.fincen.gov/sarreview082002.pdf
Suspicious Activity Report Form Preparation and Filing	1	24	http://www.fincen.gov/sarreviewforweb.pdf
Suspicious Activity Report Forms: Where to Send Completed Suspicious Activity Report Forms	6	57	http://www.fincen.gov/sarreviewissue6.pdf
Terrorist-Related Activity: How to report potential terrorist-related activity	6	53	http://www.fincen.gov/sarreviewissue6.pdf
Tips from the Regulators	6	54	http://www.fincen.gov/sarreviewissue6.pdf

Definitions and Criminal Statutes for the Suspicious Activity Report Characterizations of Suspicious Activity

In response to requests for an explanation or definition of the various characterizations of suspicious activity appearing in Item 35 of the depository institution Suspicious Activity Report form (Form TD F 90-22.47), FinCEN, with the assistance of members of the Bank Secrecy Act Advisory Group[35] SAR Feedback Subcommittee, prepared the table appearing on the following pages, which provides a listing of each category, certain Federal criminal statutes associated with the violation, and its explanation or definition. Please note that filers may select more than one type of characterization, if applicable, when completing the Suspicious Activity Report form. For example, Category C - Check Fraud and Category D - Check Kiting may be marked, or Category C - Check Fraud and Category H - Counterfeit Check may be marked.

35 The Bank Secrecy Act Advisory Group is a task force established by Congress to coordinate Bank Secrecy Act-related matters. The Bank Secrecy Act Advisory Group is comprised of high-level representatives from financial institutions, federal law enforcement agencies, regulatory authorities and others from the private and public sector.

Violation Category	Characterization of Suspicious Activity The Reportable Conditions	Possible Federal Criminal Statute(s)	Explanation/Description
a	**Bank Secrecy Act /Structuring/Money Laundering**	31 U.S.C. Section 5311 and 31 C.F.R. Part 103 Bank Secrecy Act	i. The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction recordkeeping and reporting requirement under federal law and reporting requirement under federal law ii. The transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or iii. The transaction 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 financial institution knows of no reasonable explanation for the transaction after examining the available facts including the background and possible purpose of the transaction.
		31 U.S.C. Section 5324 - Structuring Transactions to Evade Reporting	There are four types of structuring activities that are reportable: 1. To avoid generating any Currency Transaction Report, Form 8300 and supporting records, and to avoid any recordkeeping connected to monetary instruments. 2. To avoid the identification requirements, e.g. connected with non-bank money transmissions and purchase of monetary instruments. 3. To avoid suspicious detection and conventional monitoring thresholds and filters. 4. To avoid enhanced scrutiny or additional review frequently triggered by higher transaction amounts and thresholds.
		18 U.S.C. Section 1956 - Laundering of Monetary Instruments 18 U.S.C. Section 1957 - Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity	Note: 18 USC 1956 creates 3 basic categories of Money Laundering: 1. Conducting/attempting to conduct one or more financial transactions with proceeds from specified unlawful activity; 2. Transporting/transmitting/transferring one or more monetary instruments or funds into or out of the United States with intent to promote carrying out of unlawful activity, to conceal or disguise the proceeds of specified unlawful activity, or to avoid a state or federal transaction reporting requirement; 3. Where property has been represented to be from specified unlawful activity (to cover law enforcement-related sting operations where the property is really clean.) See an expanded explanation of money laundering in Section 6 of this Issue.
b	**Bribery / Gratuity**	18 U.S.C. Section 215 - Bank Bribery	Anyone who, in connection with bank business, corruptly gives, offers or promises anything of value to a bank official with the intent to influence or reward that official.
c	**Check Fraud**	18 U.S.C. Section 1344 - Bank Fraud	This type of fraud takes on many forms including: altered checks; check kiting; charge-back check fraud; closed account fraud; and variations on check forgeries. Other common check fraud violations noted are the withdrawal of funds against checks with forged endorsements or maker's signatures and counterfeit checks.

d	**Check Kiting**	18 U.S.C. Section 1344 - Bank Fraud 18 U.S.C. Section 656/657 - Embezzlement, Theft or Misapplication of Funds	A practice in which an individual with accounts at two or more financial institutions intentionally utilizes the delay in the check clearing process to write checks from one account to deposit into the second account, all the while knowing that the first account does not have collected funds. The subject continues this cycle, moving checks between accounts, to make it appear as if funds are available and using the balance in the accounts for expenditures.
e	**Commercial Loan Fraud**	18 U.S.C. Section 1344 - Bank Fraud 18 U.S.C. Section 656/ 657 - Embezzlement, Theft or Misapplication of Funds	A fraudulent loan involving a corporation, commercial enterprise, or other type of business, usually secured by some form of collateral. One example includes banks advancing loan funds to car dealers via floor plan lines of credit secured by the automobiles in inventory. Collateral is later sold, out of trust, and proceeds are not applied to the loan thus creating a loss to the lender.
f	**Computer Intrusion**	18 U.S.C. Section 1030 - Computer Fraud	A person who gains access to a computer system of a financial institution to: * Remove, steal, procure or otherwise affect funds of the institution or the institution's customers * Remove, steal, procure or otherwise affect critical information of the institution including customer account information; or * Damage, disable or otherwise affect critical systems of the institution. Note: Does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information See Issue 3, page 15, of *The SAR Activity Review* for additional information on Computer Intrusion at the following hyperlink: http://www.fincen.gov/sarreviewissue3.pdf.
g	**Consumer Loan Fraud**	18 U.S.C. Section 1344 - Bank Fraud 18 U.S.C. Section656/657 - Embezzlement, Theft or Misapplication of Funds	A loan extended to an individual for personal or household use that is obtained fraudulently. Incidents of consumer loan fraud primarily involve the submission of false or forged statements by loan applicants.
h	**Counterfeit Check**	18 U.S.C. Section 1344 - Bank Fraud	A legitimate check that is altered or forged by hand or through the use of a computer or electronic/digital device that is compromised or scanned into a computer. The payee's name, dollar amount, check serial number, and date are changed though other data (including the authorized signature) remain as they appear on the original check. The counterfeit check is purported to be genuine and negotiated.
I	**Counterfeit Credit/Debit Card**	18 U.S.C. Section 1029 - Fraud and Related Activity in Connection with Access Device 18 U.S.C. Section 1344 - Bank Fraud	A person who knowingly commits fraud by producing, using, or selling one or more counterfeit credit or debit cards. A counterfeit or fake card is created through technology to emboss stolen or fictitious card numbers, along with hologram and card issuer images, and magnetic stripes on white plastic. The cards are used for fraudulent purchases or sold to other criminals for their use.

j	**Counterfeit Instrument**	18 U.S.C. Section 1344 - Bank Fraud	The manufacture, copy, reproduction, or forgery of an instrument with the intent to defraud a financial institution. Instruments could include notes, checks, securities, bonds, certificates and other negotiable financial instruments.
k	**Credit Card Fraud**	18 U.S.C. Section 1344 - Bank Fraud	The intentional procurement of goods, services or money, without the authorization of the cardholder, credit card member or its agent, by using a stolen, lost, or cancelled credit card. May include Illegal purchases made in person, via the Internet or telephone, or through cash advances.
l	**Debit Card Fraud**	18 U.S.C. Section 1344 - Bank Fraud	The unauthorized use of a stolen, lost, or cancelled debit card for payment of goods or to acquire services or money. Debit cards are used in place of checks or cash and usually are tied to a checking account. Fraudulent use of the debit card depletes available funds in that account causing a loss to the bank customer or to the bank.
m	**Defalcation/Embezzlement**	18 U.S.C. Section 656/657 - Theft, Embezzlement, or misapplication of funds	A person who, for unauthorized personal use, embezzles, abstracts, purloins or willfully misapplies any of the moneys, funds or credits of a bank, branch, agency or organization or holding company or any moneys, funds, assets or, securities entrusted to the custody or care of such bank, branch, agency, organization, or holding company.
n	**False Statement**	18 U.S.C. Section 1001 - False Statements or entries 18 U.S.C. Section 1005 - False Entries 18 U.S.C. Section 1014 - False Statements on a Loan or Credit Application	A person who knowingly and willfully commits one of the following: 1. Falsifies, conceals or covers up by any trick, scheme or device, a material fact; 2. Makes any materially false, fictitious or fraudulent statement or representation; or 3. Makes or uses any false writing or document knowing the same to contain any materially false, fictitious or fraudulent statement or entry. The false statement must occur in a matter within the jurisdiction of a branch of the United States Government; essentially, making a false statement to a government agency when it is carrying out its mission. Section covers oral or written false statements or misrepresentations made knowingly on a loan or credit application to an insured bank (e.g., willful over-valuing of land, property, securities, or other assets or the understatement of liabilities). Such statements or misrepresentations must have been capable of influencing the bank's credit decision. Actual damage or reliance on such information is not an essential element of the offense. The statute applies to credit renewals, continuations, extensions or deferments and includes willful omissions as well as affirmative false statements. Obsolete information in the original loan application is not covered unless the applicant reaffirms the information in connection with a renewal request. The application will trigger the statute even if the loan is not made.

o	**Misuse of Position / Self Dealing**	18 U.S.C. Section 656/657 - Theft, Embezzlement, or Misapplication of Funds 18 U.S.C. Section 644 - Banker Receiving Unauthorized Deposit of Public Money 18 U.S.C. Section 215 - Bank Bribery	A person, who is not an authorized depositary of public moneys, who knowingly receives from any disbursing officer, collector of internal revenue, or other agent of the United States, public money on deposit, or by way of a loan or accommodation, with or without interest, or otherwise than in payment of a debt against the United States, or uses, transfers, converts, appropriates, or applies any portion of the public money for any purpose not prescribed by law.
p	**Mortgage Loan Fraud**	18 U.S.C. Section 1344 - Bank Fraud 18 U.S.C. Section 656/657 - Theft, Embezzlement, or Misapplication of Funds	A person who fraudulently obtains a mortgage for property or other asset primarily by the submission of false or forged statements on loan applications.
q	**Mysterious Disappearance**	18 U.S.C. Section 656/657 - Theft, Embezzlement, or Misapplication of funds	Unexplained disappearance of moneys, or other instruments of value, in bearer form, from a financial institution's branch, agency, organization, or holding company.
r	**Wire Transfer Fraud**	18 U.S.C. Section 1956 - Laundering of Monetary Instruments 18 U.S.C. Section 1343 - Fraud by Wire, Radio or Television	A person who, intending to defraud or obtain money or property by fraudulent means of false pretenses, representations or promises, transmits an electronic funds transfer.
s	**Other**		A category used to report suspicious activity that does not fit into any other violations characterization.
t	**Terrorist Financing**	18 U.S.C. 2339(a) and 18 U.S.C. 2339(b) - Harboring and Concealing Terrorists	Persons or entities who provide material support or resources to various enumerated terrorist acts, including concealing or disguising the nature, location, source or ownership of the material support or resources. Also, persons or entities providing material support or resources to designated foreign terrorist organizations, or attempting or conspiring to do so. The statute explicitly provides for extraterritorial jurisdiction, meaning it can be applied to actions occurring outside the United States.

u	**Identity Theft**	18 U.S.C. Section 1028 - Identity Theft	A person who knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under applicable state or local law. See Issue 2, page 14 of *The SAR Activity Review* for further details about identity theft at the following hyperlink: http://www.fincen.gov/sarreview2issue4web.pdf

Section 4 - Issues & Guidance

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

Guidance as to What to Do When Asked for Production of Suspicious Activity Reports

What should a financial institution do if it receives a civil subpoena that specifically asks for the production of Suspicious Activity Reports or a subpoena that, by virtue of its breadth, would encompass Suspicious Activity Reports?

If the subpoena does not specifically ask for the production of Suspicious Activity Reports, the financial institution should object to the subpoena on the grounds that some of its responsive material consists of confidential supervisory information.

If the subpoena does specifically ask for the production of Suspicious Activity Reports, the simple answer for the financial institution is to send the issuer of the subpoena a written objection referring to the regulations that have been promulgated by FinCEN and the federal regulatory agencies that state that all Suspicious Activity Reports are confidential and cannot be released.[36] For example, as set forth in the Office of the Comptroller of the Currency's regulation:

> "*SARs are confidential. Any national bank or person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed, citing this section, applicable law (e.g., 31 U.S.C. 5318(g)), or both, and shall notify the OCC.*"

36 *See* 31 C.F.R. § 5318(g)(1); 12 C.F.R. § 21.11 (pertaining to national banks); 12 C.F.R. § 208.62 (pertaining to state chartered banks that are members of the Federal Reserve System); 12 C.F.R. § 353 (pertaining to state chartered banks that are not members of the Federal Reserve System); 12 C.F.R. § 563.180(d) (pertaining to Federal thrifts and savings associations).

12 C.F.R. § 21.11(k).[37] A similar prohibition on disclosure is found in all FinCEN's Suspicious Activity Report regulations.[38] Accordingly, in addition to the suggested response above, when a financial institution receives a discovery request or a subpoena asking for the production of a Suspicious Activity Report, it should contact its primary federal regulatory agency and FinCEN (note: 31 C.F.R. 103.18(e) requires banks to notify FinCEN if they receive a subpoena covering Suspicious Activity Reports), if it is a federally-regulated bank, or FinCEN, if it is any other type of financial institution. The agencies can usually work with the institution in crafting an appropriate response. The institution should also refer to the applicable regulations, refuse to disclose any Suspicious Activity Report and, similarly, refuse to disclose whether or not a Suspicious Activity Report exists. The financial institution and its lawyer should also be careful not to disclose the existence of a Suspicious Activity Report in a response to the subpoena. Rather, the privilege log or other responsive pleading should refer generically to "nonpublic supervisory information" or something similar in nature, and not to the Suspicious Activity Report itself.

Not only does Federal law prohibit the disclosure of Suspicious Activity Reports, but 31 U.S.C. § 5318(g), as amended, provides a safe harbor from civil liability for financial institutions that disclose possible violations of law or regulation, whether the disclosures are made by filing Suspicious Activity Reports, or are made voluntarily, with the appropriate government authority.

On May 24, 2004, an Interagency Advisory was issued by the five federal regulatory agencies and FinCEN to inform financial institutions about a recent federal court case, *Whitney Nat'l Bank* v. *Karam*, 306 F. Supp.2d 678 (S.D. Tex. 2004), that reaffirms the scope of the statutory "safe harbor" protections. While the *Whitney* court ruled in a case involving a national bank and the rules and regulations of the Office of the Comptroller of the Currency, the five federal regulatory agencies and FinCEN believe that the court's rulings apply to all financial institutions that file Suspicious Activity Reports in accordance with suspicious activity reporting rules. This advisory may be found at http://www.fincen.gov/advis35.pdf and we suggest that all financial institutions familiarize themselves with the information contained therein.

On occasion, the federal banking agencies and FinCEN have filed an amicus brief or letter to the court to assist a bank that is contesting the issuance of a subpoena requiring the production of a Suspicious Activity Report. Consequently, when a financial institution is in a position of contesting such a subpoena, it should contact FinCEN and, where applicable, the banking agencies as soon as possible for further guidance.

37 *See* preceding footnote for citations to the regulations of the other Federal banking agencies.

38 *See* 31 CFR 103.17 (futures commission merchants), 103.18 (banks), 103.19 (broker-dealers), 103.20 (money services businesses), and 103.21 (casinos).

Suspicious Activity Reporting Guidelines for Reporting Advance Fee Schemes

FinCEN has received inquiries regarding whether a financial institution required to report suspicious activities pursuant to Bank Secrecy Act regulations, 31 C.F.R. Part 103, should file a Suspicious Activity Report on "4-1-9" or "advance fee fraud" schemes.

An advance fee fraud scheme typically begins when a person receives an unsolicited communication from someone in a foreign country, often Nigeria or other African nations, who purports to be a current or former official of the foreign government. The solicitation will assert an urgent need for the recipient's help to transfer a large amount of money. Explanations regarding the money's source will vary and may include proceeds from over-invoiced contracts or other contract fraud, disbursement of money from wills, sale of crude oil at below market prices, purchases of real estate, currency conversions, or winnings from an international lottery. The recipient is promised either most or all of the money to be transferred, or a substantial commission. These schemes have a common denominator–eventually the target of the scheme will be required to pay up-front (advance) fees (licensing fees, taxes, attorney fees, transaction fees, bribes, etc.) to receive the money or commission. Detailed information about these schemes is available from the United States Secret Service website, http://www.secretservice.gov/alert419.shtml.

Financial Institution Guidance on Filing Suspicious Activity Reports

If a monetary loss has not been incurred from an advance fee fraud scheme and there are no other indicators of illegal activity warranting the filing of a Suspicious Activity Report, a financial institution should not file a Suspicious Activity Report and no further action is necessary.

If a monetary loss has been incurred from an advance fee scheme or the scheme involves other indicators of illegal activity, such as investment fraud, counterfeiting, forgery, or the misuse of an official United States Government seal, a financial institution should consider filing a Suspicious Activity Report based on the requirements of 31 C.F.R. Part 103 and the Suspicious Activity Report filing instructions. In addition, the financial institution should contact the local United States Secret Service field office, local police department, or other appropriate law enforcement agency.

For general questions regarding Suspicious Activity Report filing, financial institutions should contact their primary federal regulator, self-regulatory organization, or FinCEN's Regulatory Helpline at (800) 949-2732.

Consumer Guidance

Financial institutions may direct consumers with questions regarding these schemes to the United States Secret Service website, http://www.secretservice.gov/alert419.shtml. If a consumer has incurred a monetary loss from an advance fee fraud scheme, the consumer may be directed to the local United States Secret Service field office. Contact information for field offices is available on the United States Secret Service website.

Section 5 – 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 Bank Secrecy Act within their institution. Although the Industry Forum Section provides an opportunity for the industry to share its views, the information provided may not represent the official position of regulatory authorities or FinCEN.

The Number of SAR Filings Should Not Be Determinative of an Adequate SAR Program—Quality of Program is the Goal

By John Byrne, representing the American Bankers Association (ABA) to the Bank Secrecy Act Advisory Group

Recently, several financial institutions have contacted ABA about examiner criticisms received in reviews of their Suspicious Activity Report (SAR) programs due to the number of SARs that the institution has filed. These financial institutions expressed the concern that this may reflect new criteria for evaluating the adequacy of SAR programs, namely, that the number of SARs filed meets a minimum threshold, or that institutions are not filing the same number of SARs as "peer" institutions. The concern expressed is that there be new criteria for determining the adequacy of SAR programs consisting, in large measure, of counting the number of SARs filed and, in some instances, comparing the number of SARs filed between "peer" institutions. Obviously, this would be a significant and alarming development in the examination and review process.

The continuing importance for filing SARs is to inform governmental authorities of the existence of suspicious activity that may merit further investigation by law enforcement or supervisory agencies. As was stated recently by FinCEN in the "Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative":

> *The purpose of the Suspicious Activity Report (SAR) is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the regulations of the Bank Secrecy Act (BSA). In many instances, SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases. Information provided in SAR forms also presents the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) with a method of identifying emerging trends and patterns*

associated with financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to financial institutions.

Concurrently, one of the primary, if not the most significant, reason for institutions to have adequate SAR programs is to ensure that potentially suspicious activity is appropriately identified and managed within an institution. The adequacy of a SAR program cannot be judged by the number of SAR filings, but rather must be evaluated with regard to the program's ability to identify potentially suspicious activity, evaluate whether the activity rises to the level of being suspicious requiring the filing of a SAR and, ultimately, sets a process to determine how the activity is dealt with within an institution.

The notion that the number of SAR filings can determine the adequacy of a SAR program is, by all accounts, faulty reasoning. Clearly, an institution that has not filed SARs or has a track record of minimal filings deserves closer scrutiny of its SAR program, as it may be indicative of problems within that program. However, the lack of filings or the limited number of filings should be nothing more than a signal to the supervisory agency that a closer review of the SAR program is warranted. A determination of this type should be the result of a comparison of the number of filings of a particular institution against that institution's pattern of SAR filings rather than a comparison of filings between institutions. As an example of focusing on a particular institution's SAR filings rather than comparing filings between institutions, the Federal Reserve Board instructs its examination staff to:

. . . continue the process of assuring that SARs are reviewed prior to the commencement of an examination or inspection. As the Reserve Banks have learned, a pre-examination/inspection review of SARs assists the supervisory staff in assessing compliance with the SAR requirements and provides useful information regarding potential problems that may require special attention during the course of an examination or inspection.

Fluctuations in the number of SAR filings between like or peer institutions can be attributed to numerous factors and, therefore, is not itself a viable indicator of the adequacy of a SAR program. The type of customer base that an institution maintains (for example, retail vs. corporate clientele), the markets in which an institution operates or differences in the parameters applied in monitoring customers and their transactions are all factors that may lead to differing numbers of SAR filings between institutions. Additionally, contrary guidance or direction provided to institutions by the particular functional regulator of an institution can have a significant impact on the way in which an institution views suspicious activity, affecting the number of SAR filings between institutions. (As an example, several financial institutions have reported to the ABA that examiners have instructed institutions to file SARs if they believe that they have information that may be of interest to the government, such as identifying an account or transaction related to an investigation that has appeared in the press, without regard to whether suspicious activity

actually exists.) Moreover, regulatory scrutiny of SAR filings has caused many institutions to file SARs as a defensive tactic (the "when in doubt - file" syndrome) to stave off unwarranted criticism or "second guessing" of an institution's suspicious activity determinations. The Federal Deposit Insurance Corporation, in its examination procedures, explicitly recognizes that there may be a variety of legitimate reasons for a change in the number of SARs filed:

> *Determine if the institution or any branches had significant changes in the volume or nature of SARs filed, and investigate the reason(s) for these change(s). . . (Note: Increases in SARs may be caused by an increase in high-risk customers, entry into a high-risk market or product, or an improvement in the bank's method for identifying suspicious activity. Decreases may be caused by deficiencies in the bank's process for identifying suspicious activity, the closure of high-risk or suspicious accounts, personnel changes, or the failure of the bank to file SARs.)*

With the increased focus on SAR programs and the number of SAR filings by institutions, the financial services industry is becoming increasingly concerned about the regulatory review of the SAR process. We believe that there is no correct number of SARs that should be filed in order for a determination that an institution has an adequate SAR program. A comparison between institutions of the number of SARs filed is wrong. It would be helpful if the government would re-state that SAR reporting obligations are based on an institution's analysis of potentially suspicious activity. If an institution has a SAR program that allows for a reasoned analysis of potentially suspicious activity and the institution's program is being followed, there should be no need for discussions regarding numerical threshold of SAR filings and no comparisons between institutions.

FinCEN and Regulatory Agencies Respond to Industry Forum Comments

The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration (the "agencies") and FinCEN are not aware of any specific situations where an institution has been criticized solely because the number of Suspicious Activity Reports filed did not meet a minimum threshold or for not filing the same number of Suspicious Activity Reports as "peer" institutions. It is not the policy or practice of the agencies or FinCEN to draw conclusions based solely on the number of Suspicious Activity Reports filed. Nonetheless, as evidenced by the Industry Forum article written by the American Bankers Association, there is a perception and concern within the financial services industry that examiners are criticizing institutions on this basis.

The agencies and FinCEN believe that there is no correct number of Suspicious Activity Reports that should be filed by an institution, and institutions should not be criticized solely on that basis. As part of the examination process, however, examiners must review significant changes in the volume or nature of Suspicious Activity Reports filed, and investigate the reason for this change. This may include a comparative analysis of the number of Suspicious Activity Reports filed by an institution and among peer institutions. A large discrepancy from the peer group average, or a large deviation from the number of Suspicious Activity Reports that an institution filed in the past, while not supportive of any inference or conclusion standing alone, would warrant further review by the examiners when evaluating the adequacy of an institution's Bank Secrecy Act/Anti-Money Laundering program. Financial institutions undergoing such reviews should understand that an evaluation of the volume of Suspicious Activity Reports filed is merely a tool of the examination process, and does not represent conclusions about the adequacy of the institutions' Suspicious Activity Report program.

Section 6 - Mailbag & Feedback

After the publication of each previous issue of *The SAR Activity Review*, FinCEN has provided feedback forms to enable members of the financial industries and others to provide comments, suggestions and other information about the usefulness of information contained in each edition. After the publication of *Issue 6*, FinCEN received a request from one reader, a community bank located in the Southeast, to further explain the characterization of suspicious activity category for Bank Secrecy Act/Structuring/Money Laundering (Item 35a) found on the depository institution Suspicious Activity Report form (TD F 90-22.47). The following information is provided in response to that request. Please note that the information is applicable to, not only depository institutions, but to other industries mandated to file Suspicious Activity Reports.

Review of the Bank Secrecy Act/Structuring/Money Laundering Violation on Suspicious Activity Report Forms

Money laundering is the movement of illicit funds for the purpose of concealing the true source, ownership or use of the funds. Through money laundering, the monetary proceeds derived from criminal activity are transformed into funds with an apparently legal source. Money laundering provides the fuel for drug dealers, terrorists, arms dealers and other criminals to operate and expand their enterprises. We know that criminals manipulate financial systems in the United States and abroad to further a wide range of illicit activities.

Money laundering is a well-thought out process accomplished in three stages:

> Placement: Requires physically moving and placing the funds into financial institutions or the retail economy. Depositing structured amounts of cash into the banking sector, and smuggling currency across international borders for further deposit, are common methods for Placement.
>
> Layering: Once the illicit funds have entered the financial system, multiple and sometimes complex financial transactions are conducted to further conceal their illegal nature, and to make it difficult to identify the source of the funds or eliminate an audit trail. Purchasing monetary instruments (traveler's checks, banks drafts, money orders, letters of credit, securities, bonds, etc.) with other monetary instruments, transferring funds between accounts, and using wire transfers facilitate Layering.

Integration: The illicit funds re-enter the economy disguised as legitimate business earnings (securities, businesses, real estate). Unnecessary loans may be obtained to disguise illicit funds as the proceeds of business loans.

Almost 50% of the depository institution Suspicious Activity Reports filed to date lists Bank Secrecy Act/Structuring/Money Laundering as the suspected violation. In most cases, cash deposits or exchanges represent the Placement phase. Some of the more typical activities found in the Placement phase include:

- Cash deposits of less than $10,000 begin immediately after the accounts are established and are made frequently, often daily;
- Cash deposits of less than $10,000 begin suddenly after limited or no account activity;
- Multiple cash deposits of less than $10,000 are made at a single branch location but with different tellers;
- Multiple cash deposits of less than $10,000 are made on a single banking day at different branches;
- Customer is accompanied by other individuals who each deposit cash of less than $10,000 into the same account but with different tellers;
- Cash deposits are immediately followed by wire transfers out of the account; or
- Cash deposits are followed almost immediately by withdrawals and/or checks or other monetary instruments drawn against the account for the same or similar amounts.

Cash deposits or withdrawals at dollar values of $10,000 or less or at multiple teller windows on a single banking day, at multiple branch locations or by multiple individuals into a single account on a single banking day may be indicative of structuring transactions.

Other issues that could cause suspicion at the Placement phase include:

- Cash deposits that are inconsistent with the nature of the business;
- Customer refuses to explain the source of the funds, or cancels the transaction when questioned about it;
- A business with a pattern of frequently opening and closing accounts, which receives high-levels of cash deposits that are immediately wire transferred out of the accounts;

- Cash purchase of sequentially numbered traveler's checks or money orders made in a structured amount of less than $10,000. When returned for payment, payee information of the traveler's checks or money orders is omitted or unclear;

- Electronic Benefit Transfer food stamp credits to an account followed immediately by structured cash withdrawals;

- Cash purchases of cashier's checks or other monetary instruments such as money orders in amounts under $3,000;

- Purchase of a large insurance policy with a cash premium under $10,000, followed by cancellation and refund by check; or

- Loan balance reduced by multiple cash payments.

Monetary instruments, with their easy portability and negotiability, afford money launderers opportunities for layers and layers of transactions to conceal illegal funds. Various characteristics may indicate money laundering, whether the instrument is a cashier's check, money order, foreign bank draft, or traveler's check. Samples of activity that could take place during the Layering phase include:

- Purchase of sequentially numbered traveler's checks or money orders using checks drawn on a personal or commercial bank account, cashier's checks, or other monetary instruments, possibly in structured amounts of less than $10,000. When returned for payment, payee information on the traveler's checks or money orders is omitted or unclear;

- Multiple wire transfers to multiple beneficiaries by a single individual at multiple branch or store locations;

- Multiple wire transfers to a single beneficiary conducted within minutes of each other by groups of individuals at a single remitter location;

- High dollar cash deposits followed by checks drawn against the account in similar amounts or slightly higher than the cash deposits, made payable to vendors, businesses, utilities, etc.;

- Cash deposits immediately followed by transfers to other accounts either within the same institution or at other domestic or foreign financial institutions. Transfers are accomplished by checks written off one account and deposited to another account or by electronic or online banking transfers between accounts;

- Frequent wire transfer activities to offshore locations that are not commensurate with the nature of the business or occupation of the account holder;

- Funds wired from one country to another, which are used for multiple investments, and then constantly moved to evade detection and to take advantage of foreign secrecy protections;

- Deposits of refund checks from canceled insurance policies;

- Cashier's checks exchanged for other cashier's checks in larger amounts, adding additional cash or instruments to make up the difference;

- Sending false import/export invoices overvaluing goods to move money from one company and country to another;

- Large, even-dollar wire transfers sent to offshore locations that are not commensurate with the nature of the business or occupation of the account holder; or

- Wire transfer activity by order of a company incorporated in the United States originating from its account with a foreign bank, routed through the foreign bank's correspondent account with a domestic financial institution, to a single beneficiary in yet another foreign country. Research into the "by order of company" fails to identify corporate location, officers or directors.

The final step in money laundering is the re-introduction of the laundered funds to the economy. Examples of the Integration phase are:

- Purchases of multiple certificates of deposit, on which the account holder routinely rolls over the principal each 30, 60 or 90 days and requests disbursement, by check, of only the interest on the certificates. Also, certificates of deposit purchased with illicit funds may be used as collateral for loans.

- Deposited funds used to purchase real estate, vehicles, or other property. Subsequently, those items are used as collateral for loans, creating what appear to be clean loan proceeds. Often, the loans are paid back prior to maturity with large payments of other money obtained through criminal acts. The property is then used as collateral for other laundering schemes.

- Loans secured from financial institutions with payoff dates in the far future for what appears to be legitimate business purposes, followed by the cash payoff of the principal within the first six-months of the loan period.

- Co-mingling of illicit currency with legitimate business receipts; for example, drug proceeds deposited into the account of an otherwise legitimate business and thus made to appear as normal business proceeds.

- Creating offshore, anonymous companies, which lend laundered money back to the criminal, resulting in large deposits into bank accounts in the United States.

- Selling property previously purchased by a shell company set up by the criminal.

Other examples of money laundering may be found in previously published FinCEN Advisories, *SAR Bulletins*, and editions of the *Suspicious Activity Reports – Trends, Tips & Issues*, all which may be found on the FinCEN website, www.fincen.gov. Also, some Bank Secrecy Act Examination Manuals issued by the federal financial regulatory authorities include lists of potential suspicious activity indicative of money laundering. For example, refer to Section 1001.0 of the Federal Reserve Board's *Bank Secrecy Act Examination Manual* (September 1997), www.federalreserve.gov/boarddocs/supmanual; pages 12-18 and 34-39 of the Office of the Comptroller of the Currency's *Bank Secrecy Act/Anti-Money Laundering Comptroller's Handbook* (September 2000), www.occ.treas.gov/handbook/compliance.htm as well as pages 18-21 in their booklet, *Money Laundering: A Banker's Guide to Avoiding Problems*; or Attachment 18.1 of Chapter 18 in the National Credit Union Administration's *Examiner's Guide*, www.ncua.gov/ref/examiners_guide/. The other regulatory authorities (Federal Deposit Insurance Corporation, Office of Thrift Supervision, United States Securities and Exchange Corporation, and the Internal Revenue Service) may also provide guidance to you.

It is important to note that the preceding examples are patterns that *may* indicate money-laundering activities. There may be legitimate business reasons for these transactions. However, any of the above patterns merits further investigation by the financial institution.

Financial institutions also are reminded that if they discover any suspicious activity within their institution that they know, suspect, or have reason to suspect involves the laundering of illicit funds at any phase of the money laundering process, and the dollar amount involved aggregates to their minimum reporting threshold, they should file a Suspicious Activity Report in accordance with the Suspicious Activity Report regulations. Check the appropriate violations boxes on the Suspicious Activity Report form[39] and completely and sufficiently describe the suspicious activity in the Suspicious Activity Report narrative.[40]

---

39 For Bank Secrecy Act/Structuring/ Money laundering, mark Box 35a on the depository institution Suspicious Activity Report form (TD F 90-22.47); Box 28a for money laundering and Box 28b for structuring on the Suspicious Activity Report by Money Services Business form (TD F 90-22.56); Box 30l on the Suspicious Activity Report by the Securities and Futures Industries form (FinCEN Form 101); and Box 26h for money laundering and box 26j for structuring on the Suspicious Activity Report by Casinos and Card Clubs form (FinCEN Form 102).

40 Refer to the Suspicious Activity Reporting Guidance Package for financial institutions for instructions on completing the Suspicious Activity Report narrative at http://www.fincen.gov/narrativeguidance_webintro.pdf. Additional guidance is provided to Casinos at http://www.fincen.gov/casinosarguidancefinal1203.pdf.

Feedback

FinCEN is always interested in hearing from financial institutions about the value and meaning of information conveyed in *The SAR Activity Review – Trends, Tips & Issues* and *By the Numbers*. As mentioned in the Introduction, many topics addressed in this issue resulted from requests for information submitted from financial institutions after the publication of Issue 6. ***Please, when you have concluded reading all the information contained in Issue 7, take a few moments to complete and return the Feedback form found on the next page.*** As the Introduction states, the continuing exchange of information is critical to improve the suspicious activity reporting system. Your help is vital 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 & Issues* (circle your response.)

1=Not Useful, 5=Very Useful

Section 1 - Trends and Analyses	1	2	3	4	5
Section 2 - Law Enforcement Cases	1	2	3	4	5
Section 3 - Tips on Suspicious Activity Report Form Preparation & Filing	1	2	3	4	5
Section 4 - Issues and Guidance	1	2	3	4	5
Section 5 - Industry Forum	1	2	3	4	5
Section 6 – Mailbag and Feedback	1	2	3	4	5

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

_____
_____
_____
_____

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

_____

_____

E. Did you find the Appendix / Index Listing of Previous and Current Topics useful?

Yes No

F. In May 2004, did you review and/or use *The SAR Activity Review – By the Numbers*?

Yes No

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

_____

What other statistical data would you find interesting or useful?

_____

_____

_____

G. 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 & Issues*? Please be specific - Examples might include: in a particular geographic area; concerning a certain type of transaction or instrument; other hot topics, etc.

_____

_____

_____

H. What topics would you like to appear in the next or future editions of *The SAR Activity Review – Trends, Tips & Issues?* Please be specific, i.e. automated teller machine activity conducted through indepen dently owned automated teller machines, rather than just automated teller machine activity.

_____

_____

_____

I. What questions does your financial institution have about *The SAR Activity Review* that need answering?

_____

_____

_____

J. Which of the previous issues of *The SAR Activity Review* have you read? (Check all that apply)

[ ] October 2000 [ ] June 2001 [ ] October 2001

[ ] August 2002 [ ] February 2003 [ ] November 2003

Send your Feedback Form to:

Financial Crimes Enforcement Network (FinCEN)
Fax 703-905-3698

Appendix

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

Appendix

Index of Topics from previous issues of *The SAR Activity Review*

Topic	Issue	Page	Hyperlink Address to *SAR Activity Review* Issue
Automated Teller Machine (ATM) Commonly Filed Violations	7	23	http://www.fincen.gov/sarreviewissue7.pdf
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
Broker-Dealer SARs – The First Year	7	20	http://www.fincen.gov/sarreviewissue7.pdf
Computer Intrusion	3	15	http://www.fincen.gov/sarreviewissue3.pdf
Consumer Loan Fraud	7	27	http://www.fincen.gov/sarreviewissue7.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
Food Stamp Fraud Using Electronic Benefit Transfer (EBT) Cards	7	9	http://www.fincen.gov/sarreviewissue7.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: FinCEN & Regulatory Agencies Respond to Industry Forum Comments	7	51	http://www.fincen.gov/sarreviewissue7.pdf
Industry Forum: Number of SAR Filings Should Not Determine Adequate SAR Program	7	49	http://www.fincen.gov/sarreviewissue7.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: Guidance as to What to do When Asked for Production of SARs	7	45	http://www.fincen.gov/sarreviewissue7.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 Guidelines for Reporting Advance Fee Schemes	7	47	http://www.fincen.gov/sarreviewissue7.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: 314(a) Results Enhance Material Support for Terrorism Case	7	30	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Black Market Peso Exchange	2	28	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Bank President Guilty in Loan Fraud	7	34	http://www.fincen.gov/sarreviewissue7.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: BSA Data Leads to $18 Million Seizure	7	31	http://www.fincen.gov/sarreviewissue7.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 Trafficker Forfeits Structured Cash	7	34	http://www.fincen.gov/sarreviewissue7.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: Individual Operating as Unlicensed Money Transmitter	7	30	http://www.fincen.gov/sarreviewissue7.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:	Nigerian Round-Tripping Investigation	7	33	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case:	Non-Profit Organization Operating as Illegal Money Remitter	7	31	http://www.fincen.gov/sarreviewissue7.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 Scheme	2	26	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case:	Ponzi Scheme	7	31	http://www.fincen.gov/sarreviewissue7.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:	Telemarketing Fraud	7	33	http://www.fincen.gov/sarreviewissue7.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:	Unlicensed South American Money Exchanger	7	32	http://www.fincen.gov/sarreviewissue7.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 & Feedback – Review of BSA/Structuring/Money Laundering Violation on SAR Forms	7	53	http://www.fincen.gov/sarreviewissue7.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
Refund Anticipation Loan (RAL) Fraud	7	15	http://www.fincen.gov/sarreviewissue7.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 Tips: Computer Intrusion and Frequently Asked Questions	3	38	http://www.fincen.gov/sarreviewissue3.pdf
SAR Tips: Definitions and Criminal Statutes for SAR Characterizations of Suspicious Activity	7	39	http://www.fincen.gov/sarreviewissue7.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: How do I . . .?	7	38	http://www.fincen.gov/sarreviewissue7.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: SAR Guidance Package	7	37	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Special Guidance Related to Identity Theft and Pretext Calling	2	34	http://www.fincen.gov/sarreview2issue4web.pdf
SAR Tips: Suspicious Activity Reporting Guidance for Casinos	7	37	http://www.fincen.gov/sarreviewissue7.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	7	35	http://www.fincen.gov/sarreviewissue7.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
Suspicious Endorsed/Third-Party Checks Negotiated Abroad	7	11	http://www.fincen.gov/sarreviewissue7.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
USA PATRIOT Act 314(a) Progress Report (February 2003 – October 2003)	6	37	http://www.fincen.gov/sarreviewissue6.pdf
USA PATRIOT Act 314(a) Progress Update (February 2003 – May 2004)	7	29	http://www.fincen.gov/sarreviewissue7.pdf
Use of Traveler's Checks to Disguise Identities	3	22	http://www.fincen.gov/sarreviewissue3.pdf
Use of U.S.-Based Shell Corporations and Foreign Shell Banks by Eastern Europeans to Move Money	7	3	http://www.fincen.gov/sarreviewissue7.pdf
Voluntary SAR Filings	3	26	http://www.fincen.gov/sarreviewissue3.pdf
Voluntary SAR Filings	2	19	http://www.fincen.gov/sarreview2issue4web.pdf