

The background of the cover is a dark teal color. A large, faint, circular seal of the Financial Crime Enforcement Bureau (FCEB) is centered. The seal contains the text "FINANCIAL CRIME ENFORCEMENT BUREAU" around the top and "DEPARTMENT OF JUSTICE" around the bottom. In the center of the seal is a globe with binary code (0s and 1s) overlaid on it. The text "ADMINISTERING BANK SECRECY ACT THROUGH GUIDANCE" is written along the inner edge of the seal, and "BANK SECRECY ACT DATA TO IDENTIFY TERRORISM" is written along the outer edge. The text "Issue 10" is prominently displayed in the upper left quadrant of the cover.

Issue 10

May 2006

The SAR Activity Review

Trends, Tips & Issues

The SAR Activity Review

Trends

Tips &

Issues

Issue 10

Published under the auspices of the BSA Advisory Group

May 2006

Table of Contents

Introduction	1
Section 1 – Director’s Forum	3
Section 2 – Trends and Analysis	
Suspicious Activity Reports: Filing Activity and Detection of Unlicensed/Unregistered Money Services Businesses.....	5
Highlighted Trend: Mortgage Loan Fraud.....	13
Section 3 – Law Enforcement Cases	
Bank Secrecy Act Data is an Integral Component of the Federal Bureau of Investigation’s Geographic Information Mapping Technology.....	17
Investigations Assisted by Bank Secrecy Act Data.....	19
Section 4 – Tips on SAR Form Preparation & Filing	
Suspicious Activity Report Form Completion Tips – A Trend Analysis of Frequently Asked Questions Received on FinCEN’s Regulatory Helpline.....	33
Section 5 – Issues & Guidance	
Money Services Business Registration and De-Registration.....	39
Grand Jury Subpoenas and Suspicious Activity Reporting.....	42
When Does the 30-Day Time Period in Which to File a Suspicious Activity Report Begin?.....	44
Section 6 – Industry Forum	
Bank Secrecy Act Compliance by the Money Services Business Industry.....	47
Section 7 – Feedback Form	53
Appendix – Index of Topics from Current and Previous Editions of <i>The SAR Activity Review – Trends, Tips & Issues</i>	

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 agencies¹ to provide meaningful information about the preparation, use, and value of Suspicious Activity Reports (SARs) filed by financial institutions.

In response to your feedback, we have expanded the descriptions of law enforcement cases included in Section 3 to better demonstrate how integral Bank Secrecy Act (BSA) data is to the law enforcement community. As you will read, many of these cases, which range in topic from drug investigations to insurance fraud, were proactively initiated as a result of your BSA report filings. We are confident that the additional details provided in these cases will add more value for our readers.

This edition’s theme is the role of SARs in the Money Services Business (MSB) industry. The articles in this issue detail emerging topics such as how to register/de-register an MSB, using SARs to detect unregistered MSBs, the increasing frequency of SARs indicating mortgage loan fraud, and filing SARs after being served with a grand jury subpoena. Below is a detailed view of topics discussed in this issue.

- Section 1: Director’s Forum;
- Section 2: Trends and Analysis – SARs related to unregistered/unlicensed MSBs as reported by depository institutions and mortgage loan fraud;
- Section 3: Law Enforcement Cases – an example of how the Federal Bureau of Investigation (FBI) is utilizing BSA data to investigate terrorist financing cases and summaries of BSA data used in criminal investigations;

1 Participants 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; Board of Governors of the Federal Reserve System; Office of the Comptroller of the Currency; Federal Deposit Insurance Corporation; Office of Thrift Supervision; National Credit Union Administration; U.S. Department of Justice’s Criminal Division and Asset Forfeiture & Money Laundering Section and the Federal Bureau of Investigation; U.S. Department of Homeland Security’s Bureau of Immigration and Customs Enforcement and U.S. Secret Service; U.S. Department of the Treasury’s Office of Terrorism and Financial Intelligence, Internal Revenue Service, and the Financial Crimes Enforcement Network.

- Section 4: Tips on Form Preparation and Filing – the most frequently asked questions received by FinCEN’s Regulatory Helpline related to proper preparation of a SAR;
- Section 5: Issues and Guidance – details on MSB registration and de-registration; guidance about whether, when and how a financial institution should file a SAR after being served with a grand jury subpoena; and guidance on when a SAR must be filed;
- Section 6: Industry Forum – focuses on SAR filing and risk assessment within the MSB industry;
- Section 7: Feedback Form.

Your comments and feedback are important to us. Please take a moment to let us know if the topics chosen are helpful. As noted above, we have included a feedback form in Section 7.

Your comments may be addressed to either or both of *The SAR Activity Review* project co-chairs:

John J. Byrne
Senior Vice President
AML Strategies
Bank of America
730 15th Street, 1st Floor
Washington, DC 20005
(202) 624-4814 (phone)
(202) 746-2455 (cell)
john.j.byrne@bankofamerica.com

Deborah F. Silberman
Regulatory Policy and Programs Division
Financial Crimes Enforcement Network
P. O. Box 39
Vienna, VA 22183-0039
(FinCEN)
(202) 354-6031 (phone)
Deborah.Silberman@fincen.gov or
sar.review@fincen.gov

Section 1 - Director's Forum



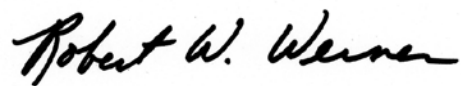
I am pleased to introduce the tenth edition of *The SAR Activity Review*. The focus of this edition is the MSB industry. Article topics include the use of SARs to detect unregistered MSBs and guidance on registration and de-registration of a business as an MSB. The industry forum article addresses transaction monitoring and reporting for MSBs. I hope you will find value in the discussion of these matters, as well as in the law enforcement cases and other articles in *The Review*.

I want to take this opportunity to affirm my commitment to our duty to support law enforcement efforts and to foster interagency and global cooperation against domestic and international financial crimes through the efficient and effective collection, analysis and sharing of information. The information collected by FinCEN not only provides law enforcement, intelligence, and regulatory agencies with leads indicative of illicit activity, it also provides the data for identifying trends and patterns, vulnerabilities and compliance-related deficiencies. To accomplish these goals, we will continue to explore methods by which we can enhance the ability of our law enforcement and regulatory colleagues to access and analyze BSA data.

I also want to reaffirm my commitment to expanding and improving outreach to and communication with our diverse constituencies in the financial services sectors and our federal and state regulatory colleagues on issues of mutual interest. I anticipate that the cooperation among these constituencies will continue to be exceptional. One extremely important tool for tackling concerns on a collaborative basis is the BSA Advisory Group. The Advisory Group provides a forum through which industry, regulators and law enforcement can surface issues, participate in candid discussion, and provide recommendations for productive and creative resolutions.

Another valuable resource for the industry is the ability voluntarily to share information pursuant to the provisions of section 314 of the USA PATRIOT Act. In particular, under regulations implementing section 314(b), financial institutions may share information regarding individuals, entities, organizations and countries for purposes of identifying or reporting activities

that the institutions suspect may involve possible terrorist activity or money laundering. The statute and regulations provide a safe harbor from liability to financial institutions that share information pursuant to section 314(b). The potential to network information about possible suspects and money laundering or terrorist financing activities, and the efficiencies that could be achieved thereby, are enormous. I encourage financial institutions to develop that potential through a more robust use of the 314(b) process. We stand ready to facilitate that effort in any way that we can, thereby helping to fulfill the common mission of safeguarding our financial system from the abuses of financial crime.

A handwritten signature in black ink that reads "Robert W. Werner". The signature is written in a cursive, flowing style.

Robert W. Werner
Director, Financial Crimes
Enforcement Network

Section 2 - Trends and Analysis

This section of *The SAR Activity Review* describes patterns identified in suspicious activity reporting by both depository and non-depository institutions. In this issue, we address suspicious activity reporting related to unlicensed/unregistered MSBs and mortgage loan fraud.

Suspicious Activity Reports: Filing Activity and Detection of Unlicensed/Unregistered Money Services Businesses

An initial analysis of suspicious activity reporting by depository institutions identifying potentially unregistered/unlicensed MSBs underscores the need for further guidance on characteristics that may indicate MSB activity through account relationships.

In 1999, the Financial Crimes Enforcement Network (FinCEN) extended the BSA regulatory regime to MSBs, that is, certain non-bank financial institutions that engage in a variety of financial services. A person or other entity that qualifies as an MSB,² whether or not licensed as such by a State, must register with FinCEN³ and, as part of that registration, maintain a list of any agents. In addition, each MSB is required to establish and implement an anti-money laundering program. Most MSBs are required to (and others are encouraged to voluntarily) file a SAR regarding any transaction or pattern of transactions conducted or attempted by, at, or through the MSB that is suspicious and involves or aggregates funds or assets of at least \$2,000 if the MSB knows, suspects, or has reason to suspect that the

- 2 Under 31 C.F.R. § 103.11(uu), the definition of MSB includes each agent, agency, branch, or office within the United States doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities; (1) currency dealer or exchanger; (2) check casher; (3) issuer of traveler's checks, money orders or stored value; (4) seller of traveler's checks, money orders or stored value; (5) money transmitter, regardless of the amount of money transfer services offered; and (6) the U.S. Postal Service, except with respect to the sale of postage or philatelic products. A person who does not offer one or more of the financial services specified in (1) through (4) above in an amount greater than \$1,000 in currency or monetary or other instruments for any person (in one type of activity) on any day in one or more transactions is not included in the definition of an MSB. For additional information, see 31 C.F.R. § 103.11(uu) and www.msb.gov.
- 3 Currently, the regulation requiring the registration of MSBs does not apply to the U.S. Postal Service, to agencies of the United States, of any State, or of any political subdivision of a State, or to a person to the extent that the person is an issuer, seller, or redeemer of stored value. (See 31 C.F.R. §103.41(a)).

transaction or transactions; is derived from illegal activity or intended to hide or disguise funds or assets derived from illegal activity; is designed to evade the requirements of the BSA, whether through structuring or other means; serves no business or apparent lawful purpose and the MSB knows of no reasonable explanation for the transaction after examining all available facts; or involves use of the MSB to facilitate criminal activity.⁴

Given the growth in number of MSBs, including the ancillary provision of such services, we are working to ensure that these businesses comply with federal registration, anti-money laundering program, and recordkeeping and reporting requirements. To that end, we have begun to study relevant SARs so that we may understand how, and the extent to which, banks and other financial institutions identify potentially unregistered MSBs. The first phase of this study examined depository institution SARs filed between January 1, 2002 and April 30, 2005. The findings from that study, involving 1,214 SARs, are presented herein.

On April 26, 2005, FinCEN, along with the federal banking agencies, issued interagency interpretive guidance to depository institutions on providing banking services to MSBs operating in the United States⁵ (Interagency Guidance). In that guidance, we specifically directed depository institutions to file SARs on businesses that are unregistered or unlicensed MSBs. We also stated that the guidance was not “a directive to banking organizations to conduct immediately a review of existing accounts for known MSBs for the sole purpose of determining licensing or registration status.” FinCEN and the federal banking agencies’ expectations have not changed in this regard. The Interagency Guidance has been incorporated into the Federal Financial Institutions Examination Council’s (FFIEC’s) 2005 *BSA/Anti-Money Laundering Examination Manual*.⁶

Preliminary research reveals that between May 1, 2005 and February 28, 2006, depository institutions filed an additional 2,934 SARs related to suspected unregistered MSB activities. The filing volume during this ten-month period reflects a 142 percent increase over the more than three-

4 See, generally 31 C.F.R. § 103.20. Special note concerning issuers of money orders and traveler’s checks: issuers are only required to report transactions or patterns of transactions that are suspicious and involve or aggregate funds or other assets of at least \$5,000 if identification of those transactions is derived from a review of clearance records or other similar records in connection with items sold or processed. 31 C.F.R. § 103.20(a)(3).

5 See “Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States,” (April 26, 2005) available at <http://www.fincen.gov/guidance04262005.pdf>.

6 An electronic version of the *FFIEC BSA/AML Examination Manual* may be found at http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

year period of January 1, 2002 through April 30, 2005 (e.g., prior to the issuance of the guidance). We are continuing to analyze the May 1, 2005 through February 28, 2006 filings to identify specific individuals and entities operating as unregistered MSBs for possible regulatory follow-up action or, if necessary, referral to law enforcement. We plan to use information from both studies to continue developing guidance for financial institutions that contributes to better identification and reporting of unregistered MSBs. The results of our further study will be published in a subsequent edition of *The SAR Activity Review*.

Depository Institutions--Types of Activities Observed

FinCEN's research identified 1,214 relevant depository institution SARs filed between January 1, 2002 and April 30, 2005. Analysis of these documents identified 1,017 businesses and 305 individuals apparently engaged in unregistered MSB-related activities.⁷

Analysis of the narrative sections of the relevant depository institution SARs found reference to at least 13 different types of MSB-related activities.⁸ When studying these SAR narratives for patterns, the sampling revealed check cashing—both over \$1,000 for a customer on any day and non-specific—as the activity most often reported, followed by money transmission (as illustrated in Table 1 below). Most notably, 15 SARs involved either indictments or arrests for alleged criminal behavior associated with the operation of the MSB or concerned activities strongly suggesting specific criminal activities.

For example, three SARs filed by three separate depository institutions reported the indictment of a corporation for acting as an unlicensed funds transmitter. This corporation sent over \$3.2 billion from shell companies to offshore accounts over a five-year period beginning in 1997.

Another SAR narrative described a company whose owner was arrested in late 2004 for operating as an unlicensed money transmitter. This individual made frequent deposits to his company's account, usually through several small checks. The owner subsequently sent two or three funds transfers

7 Entities and individuals identified in SARs were compared with the most recent Money Services Business Registration List. FinCEN refers entities determined to be operating as unregistered MSBs to the appropriate regulatory or law enforcement agency.

8 Some SAR narratives described multiple MSB-related activities.

a month to beneficiaries located in India, Hong Kong, and South Africa. Indications are that this was a hawala-type⁹ operation involved in sending money either directly to India, or alternately to Hong Kong or South Africa to purchase gold to be subsequently smuggled into India.

A third SAR narrative described a customer's use of two different business accounts to transfer hundreds of thousands of dollars. The bank believed that the pattern of funds transfers indicated a fraudulent investment scheme. Bank research determined the customer had been arrested in the early 1990s on fugitive warrants from three different states for fraud-related charges.

9 Hawala is a type of informal value transfer system based on trust that exists and operates outside of, or parallel to mainstream banking or financial channels and through which money can be made available internationally without actually moving it. See FinCEN Advisory Issue 33 "Informal Value Transfer Systems" (March 2003). This activity is not illegal in the United States unless the operation fails to comply with federal and state regulations pertaining to money transmitters, including regulations under the BSA.

Table 1: Types of Reported Activities

Activity	Occurrences	Percentage of Total Reported Activities
Check cashing (Over \$1,000 aggregate for any person on any day)	345	27.87%
Check cashing (Non-specific)	339	27.38%
Money transmission	309	24.96%
Money services businesses activities (Non-specific)	131	10.58%
Informal Value Transfer Systems (Including hawala)	49	3.96%
Arrests, indictments, and illicit activities associated with the operation of unregistered money services business	15	1.21%
On Money Services Business Registration List without authorization date	13	1.05%
No apparent money services business activity	13	1.05%
Money laundering	12	0.97%
Currency exchange	7	0.57%
Black Market Peso Exchange-like activity	2	0.16%
Exchange of cashed third-party checks with related business for cash	2	0.16%
Registered money services business facilitating transfers for related unregistered money services business	1	0.08%
TOTALS	1,238	100.00%

Check Cashing and Money Transmitting

Table 2 identifies the top 15 states where subjects were identified as unregistered check cashers¹⁰ whose check cashing transactions exceeded \$1,000 per day for any person, singly or in aggregate. This table also displays the top 15 states where suspects engaged in unregistered money transmission, as measured by numbers of SARs filed.

¹⁰ These top 15 states were determined from the 345 instances reported in Table 1.

Table 2: Top 15 Filer States

State	Number of Check Cashers (> \$1,000)	Percentage of Total Reports of Check Cashers (>\$1,000)	Number of Money Transmitters ¹¹	Percentage of Total Reports of Money Transmitters
Alabama	7	2.03%	6	2.02%
Arizona	12	3.48%		
California	18	5.22%	80	26.94%
Colorado	11	3.19%		
Connecticut			6	2.02%
Delaware			6	2.02%
Florida	9	2.61%	12	4.04%
Georgia	7	2.03%		
Illinois	19	5.51%	9	3.03%
Indiana	11	3.19%		
Massachusetts			11	3.70%
Michigan	34	9.86%		
New Jersey			23	7.74%
New York	15	4.35%	22	7.41%
Ohio	64	18.55%	11	3.70%
Oregon			8	2.69%
Tennessee	22	6.38%	8	2.69%
Texas	32	9.28%	19	6.40%
Virginia			9	3.03%
Washington	11	3.19%	23	7.74%
Wisconsin	8	2.32%		
TOTALS	280	81.19%	253	85.17%

Results of this analysis revealed unregistered check cashers to be most concentrated in the central United States (Ohio, Michigan, Texas, Tennessee, and Illinois), whereas unregistered money transmitters were found to be most concentrated on the East and West coasts (California, Washington, New Jersey, New York, and Florida).

¹¹ 297 SARs of the 309 reported with this activity provided state locations for suspects.

Informal Value Transfer Systems

A total of 49 SARs were identified which described activities consistent with hawala and other informal value transfer systems. One SAR was the latest in a series of SARs filed on a purported student who made numerous cash deposits totaling over \$1.1 million during an eight-month period beginning in 2004 and then sent periodic wire transfers to an apparent relative in the Far East.

In another instance, an individual deposited numerous \$500 money orders into his account and subsequently wrote checks totaling over \$300,000, which were then negotiated in a Middle Eastern country.

Probable Money Laundering—Narratives Indicate Individuals Suspected of Engaging in Structuring and/or Unlicensed/Unregistered Money Transmitting

Table 1 references 12 unregistered MSB-related SARs that concern activities linked to suspected money laundering. One reported an individual who received over \$500,000 in wire transfers on a specific date in early 2005 and also purchased cashier's checks totaling \$450,000. The next day he re-deposited one of the checks for \$200,000 and issued 21 checks for \$9,000 all to the same payee. These actions may be evidence of possible tax evasion or laundering of illicit proceeds. Issuance of the \$9,000 checks also suggests they were intended to be cashed in a structured manner to evade currency transaction reporting requirements.

Another SAR reported an individual who structured cash deposits into a personal account to transact same-day wire transfers to the same beneficiary located in Central America. The deposits totaled more than \$100,000 and the wire transfers exceeded \$145,000. The money was allegedly for craft items; however, a site visit to the individual's business by employees of the reporting institution cast doubt on whether the business activity could support the volume of purchases. In addition to the possibility of operating as an unregistered money transmission business, the business may also be engaged in laundering illicit receipts from unidentified sources.

Multiple Financial Institutions Reporting Suspicious Activities on the Same Suspect

In several instances, multiple financial institutions reported suspicious activities by the same or possibly the same suspect. Two SAR narratives described a Southwest-based food market that was reported by two financial institutions located in different states outside the region. Each bank filed a SAR indicating funds transfers from one country in the Middle East to another.

In another instance, a bank filed a SAR on and closed the account of an individual who admitted to acting as an unregistered funds transmitter. Apparently undeterred by the closure of the account, the individual continued to operate as an unregistered funds transmitter. Subsequently, another bank filed a SAR identifying an individual with the same name as having been indicted for operating an unregistered MSB. This is a good example of the potential value of SAR narratives to law enforcement. The first bank's filing may have provided a lead to law enforcement and helped establish the level of the suspect's awareness of the legality of the activities that the suspect was conducting.

In the same vein, another bank reported that the signer on a business account admitted that the business was operating as an unregistered funds transmitter. Significantly, another bank reported later that the same business continued to engage in this activity.

Bank Secrecy Act Compliance

FinCEN is continuing to assess the impact of the Interagency Guidance.¹² Initial statistics from the post-guidance portion of the study suggest that, while the Interagency Guidance may have caused a significant increase in filings, the largest 15 filers continued to produce approximately the same percentage of filings (68 percent pre-guidance and 66.25 percent post-guidance).¹³

The study found that SAR narratives written by 13 of these 15 depository institutions appeared clear and detailed. Of the two remaining institutions, one did not provide sufficient information to determine whether customers engaging in check cashing were breaching the \$1,000 per person per day check cashing threshold. The other institution failed to specifically identify *any* activities that would qualify the subject of the report as an unregistered MSB.

Conclusion

The relatively small number of SARs filed between January 1, 2002 and April 30, 2005 that identified potentially unregistered MSBs was one factor, among many, for including a clear statement in the Interagency Guidance on the need for banks to file SARs on unregistered MSBs. We believe that there continue to be MSBs operating without required registration or licensing and that such businesses need banking services to operate.

12 Prior to the issuance of the Interagency Guidance, the 15 largest depository institutions filed approximately 68 percent of all SARs located during the study describing activities consistent with the operation of an unregistered MSB.

13 The statistics for post-guidance filings are based on raw numbers and are subject to change once methodologies used in the pre-guidance study are applied to the data in the post-guidance study. These results will be reported in a future issue of *The SAR Activity Review*.

Additional guidance focusing on ways to recognize potentially unregistered MSBs is one of a number of approaches that may help to address the issue. While we believe the Interagency Guidance provides evidence that this approach is useful, it is difficult to draw conclusions about direct causality between the Interagency Guidance and the increased volume of SARs reporting unregistered MSBs filed subsequent to the Interagency Guidance. Evidence suggests that the increase in filings may be more indicative of banks addressing a range of BSA compliance issues as a result of ongoing dialogue between industry and regulators, which resulted in a look-back and reporting of previously unidentified or unreported suspicious activity. Further, increased filings may be attributable to institutions strengthening their compliance programs through improved training and to an improvement in monitoring systems because of technological innovations.

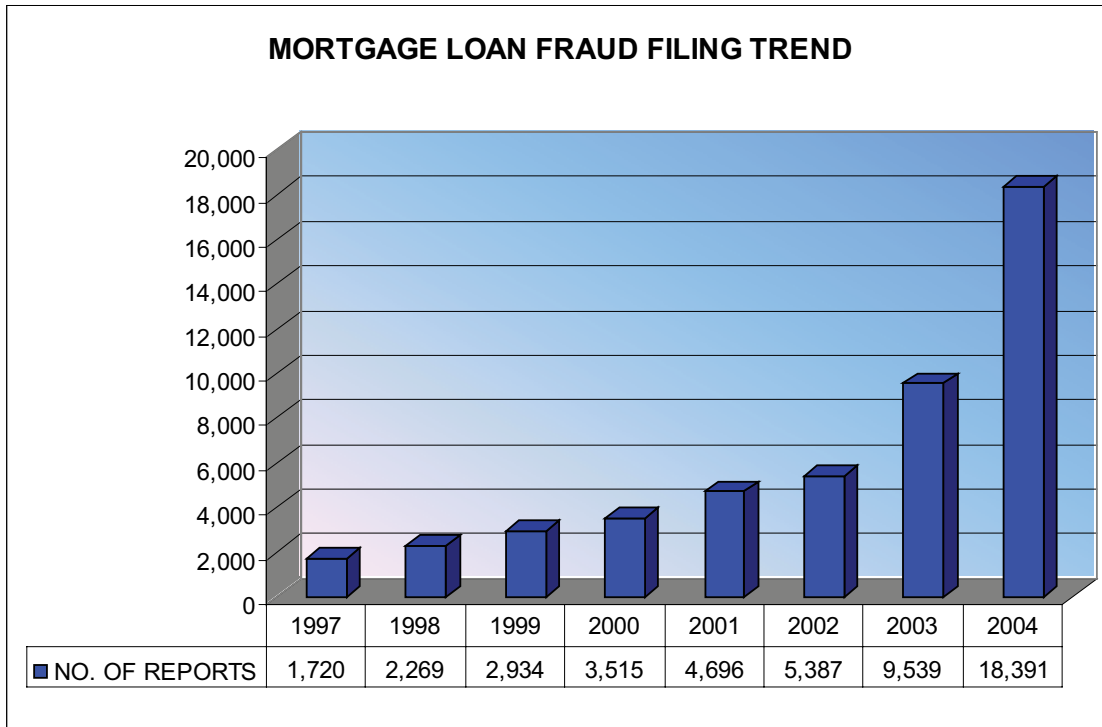
FinCEN will continue to study this issue and will report the results from the recent analytical study of those filings in Issue 11 of *The SAR Activity Review – Trends, Tips & Issues*. We also will continue to develop appropriate guidance designed to assist financial institutions in identifying and reporting potentially unregistered MSBs.

Highlighted Trend: Mortgage Loan Fraud

FinCEN conducted research on SARs filed by depository institutions reporting mortgage loan fraud as the violation (in whole or in part). The complete results of FinCEN's study will be made available in a separate publication. The following represents a portion of the wide-ranging findings contained in the report:

Between 1997 and 2004, SARs filed by depository institutions reporting mortgage loan fraud increased by 969 percent. This trend continued with 11,509 reports of mortgage loan fraud filed in the first six months of 2005 alone.

Table 3: Depository Institution SARs Involving Mortgage Loan Fraud/Annual Filing Trends January 1, 1997 to December 31, 2004



Monetary Value Involved

The total dollar amount of suspicious activity reported for the period between April 1, 1996 and June 30, 2005 was \$16,748,111,493. In July 2005, the national median price for existing homes for all housing types was \$218,000, according to the National Association of Realtors. Over 58 percent of the mortgage loan fraud reports fell into the range between \$100,001 and \$500,000.

Seven of the top ten SAR filers in this study reporting mortgage loan fraud also were listed in the top three percent of 1,506 nationally ranked U.S.-chartered commercial banks with consolidated assets of \$300 million or more.¹⁴ However, this could be due to their market share in mortgage lending.

¹⁴ Board of Governors of the Federal Reserve System Internet site, <http://www.federalreserve.gov/releases/lbr/current/default.htm>, (accessed October 3, 2005), Insured U.S.- Chartered Commercial Banks that Have Consolidated Assets of \$300 Million or More, Ranked by Consolidated Assets as of December 31, 2005.

Mortgage Fraud Hot Spots

The Federal Bureau of Investigation (FBI) reports that 26 states have significant mortgage loan fraud problems.¹⁵ The FBI indicates that the top 10 “hot spots for mortgage fraud are California, Colorado, Florida, Georgia, Illinois, Michigan, Missouri, Nevada, South Carolina, and Utah.” This ranking is based on the number of active federal law enforcement cases involving mortgage loan fraud. SARs indicate that the largest concentration of fraud is found in the entire eastern region of the United States. Other “hot spots,” according to those filings, include Arizona and Texas. Enacted and proposed laws aimed at thwarting mortgage loan fraud are a step in the right direction.

Top Suspect Occupations Associated with Mortgage Loan Fraud Reported

- Finance-related occupations were the most commonly reported suspect occupation associated with mortgage loan fraud with 8,345 (13.62 percent) filings. Accountants, mortgage brokers, and lenders were included as finance industry occupations.
- Business-related occupations were the next highest reported suspect occupation associated with mortgage loan fraud with 3,455 (5.64 percent) filings.

Types of Fraudulent Mortgage Loan Activity Reported

- Falsification of the Loan Application was described in 543 (nearly 52 percent) of the sampled narratives.
- Identity Theft/Fraud was described in 225 of the sampled narratives (21 percent).
- Misrepresentation of Loan Purpose or Misuse of Loan Proceeds was described in 142 of the sampled narratives (14 percent).
- Appraisal Fraud was described in 100 of the sampled narratives (9.5 percent).
- Fraudulent Flipping was specifically identified in 22 of the sampled narratives (2 percent).

¹⁵ U.S. Department of Justice, Federal Bureau of Investigation, Financial Crimes Section, Financial Crimes Report to the Public, “*Mortgage Loan Fraud*”, D12, May 2005, http://www.fbi.gov/publications/financial/fcs_report052005/fcs_report052005.htm. (Accessed September 28, 2005).

- Fraud involving Multiple Loans was described in 15 of the sampled narratives (1.4 percent).

Vulnerabilities

- Modern technology such as the Internet, while providing an easy means to submit loan applications, also helps fuel increased mortgage loan fraud by allowing criminals to commit fraud while their identities remain shielded.
- Increased use of third-party brokers has created opportunities for organized fraud groups.
- The lack of standard regulations and educational or experience criteria for mortgage loan brokers appears to contribute, in part, to the growth of mortgage loan fraud.

Section 3 – Law Enforcement Cases

This section of *The SAR Activity Review* affords law enforcement agencies the opportunity to summarize investigations where SARs and other BSA information played an important role in the successful investigation and prosecution of criminal activity. This issue includes an example of how the Federal Bureau of Investigation is using BSA data to investigate terrorist financing cases, as well as new case examples from federal, state and local law enforcement agencies. Additional law enforcement cases can be found on the FinCEN website, www.fincen.gov, under the Law Enforcement/LE Cases Supported by BSA Filings link. This site is updated periodically with new cases of interest.

Bank Secrecy Act Data is an Integral Component of the FBI's Geographic Information Mapping Technology

U.S. law enforcement and regulatory agencies give priority to detecting terrorist financing. In particular, they seek to identify individuals or businesses used as fundraising vehicles and to detail the movement of financial assets. Effectively implementing strategies that prevent, disrupt and stop the ability of terrorist financing operations requires the coordination and organizational analysis of both financial data and intelligence gathered by law enforcement. Maximizing the types of financial data available to law enforcement significantly enhances the value of law enforcement investigations and assessments. While each individual financial record provides relevant information, examining numerous records over a period of time gives law enforcement a better understanding of possible violations and investigative opportunities.

BSA data filed everyday by depository institutions, casinos, insurance companies, and MSBs accounts for a tremendous amount of financial information that is essential to tracing and identifying potential avenues of terrorist financing. The data extracted from BSA filings is extremely useful in identifying and linking investigative information and intelligence with ongoing investigations, as well as in identifying leads for new investigations. Although data from a single report often has minimal investigative value,

when examined and compared with other BSA data and other intelligence, the significance of a report, or a single element of that report, is often greatly increased.

Currently, FinCEN provides the FBI with access to electronic copies of BSA filings to be imported into a FBI data warehouse. This platform allows specific data fields to be extracted and compared against investigative information and intelligence collected by the FBI and other agencies. Some of the information that is compared and examined includes names, Social Security numbers, dates of birth, passport numbers, addresses, business names and account numbers. A recent examination of millions of BSA documents revealed over 80,000 specific filings with some relationship to subjects of terrorism investigations.

The FBI has developed several technologies enabling them to exploit extracted BSA data by using computer software that presents visual patterns of various entities or groups involved in potential criminal activities through link analysis charts, graphs, and other customized technologies. One such technology allows the FBI to display certain characteristics of BSA data on generated maps, which can be zoomed in as far as the street level. The users of this technology specify the characteristics of BSA data that they want represented, such as suspect name, suspect address and bank address. They may choose to incorporate other internal information that is available to complete the search query. The users then map the compiled data.

This type of mapping technology allows for common tasks as well as complex operations. It also permits previously mapped and analyzed datasets to be merged and updated. Geographic information mapping technology is evolving and provides the FBI with better methods of analysis by identifying trends and patterns and managing and organizing the data. The benefits of providing a visual geographic summary of the captured data are numerous and allow the FBI to communicate important and viable data to their respective audiences.

With the continuing advances in technology, the FBI and other law enforcement agencies are better equipped to review and analyze BSA data. To date, the results of these analyses continue to underscore the tremendous value of BSA data as a significant source of financial intelligence.

Investigations Assisted by Bank Secrecy Act Reporting

Proactive Bank Secrecy Act Search Leads to Arrest in Ponzi Scheme

In 2005, a financial investigator discovered a SAR filed two weeks earlier that referenced an investment group and a potential Ponzi scheme. The investigator contacted the bank and received supporting material related to the SAR. Because of the suspicious activity, the bank was preparing to close the account.

The District Attorney's office quickly launched an investigation. In total, there were four separate SARs that financial institutions submitted on the defendant documenting actions that had the appearance of a Ponzi scheme. In addition, there were several Currency Transaction Reports (CTRs) related to the defendant that recorded additional transactions that were part of the scheme.

The defendant had promised investors outlandish interest rates, up to 100 percent annually. He deceived customers by lying to them about his investment experience, the legality of the business, and the way that a customer's money would be invested. The defendant told investors, among other things, that he was a highly experienced investor, when in reality the defendant had no investment experience whatsoever.

Although the dollar amount of the suspected criminal violations was somewhat lower than most of their cases, the nature of the possible crime hastened their action. Investigators believed that if they did not act immediately, the perpetrator might defraud more victims. The District Attorney executed a search warrant and arrested the individual listed on the SAR.

A grand jury convened and handed down 18 felony counts, including multiple counts of fraud, larceny, and money laundering. The defendant pleaded guilty to the charges. The subject will serve a minimum of two to seven and a half years in prison, although the final sentence will be determined based upon the amount of restitution provided.

(Investigating Agency: State District Attorney)

Currency Transaction Reports Expose Drug Traffickers Laundering Profits Through Casinos

Nine members of a drug trafficking organization were exposed and convicted largely through evidence collected from CTRs.

The defendant was known as the “money-man” of the drug trafficking organization because he was responsible for laundering the organization’s illegal proceeds from drug sales. The defendant was a known, though modest, gambler until hired by the drug trafficking organization to launder its profits. Both the money the organization paid the defendant for these services and the large sums of money put into the defendant’s possession to be laundered allowed the defendant to trade a low-budget gambling style for that of a high roller.

The defendant would recruit third parties at a casino to purchase or cash in chips for the defendant, paying these recruits a nominal fee for doing so. Presumably unbeknownst to the recruits, the chips were purchased with illegal drug profits. After spending some time gambling, the defendant would cash out some of the chips, claiming they were gambling winnings, and thereby fabricating a source for the group’s revenue other than drug trafficking, thus successfully “laundering” the money.

Every time the defendant cashed-out chips in an amount over \$10,000, the transactions were recorded on a CTR by the casino. According to the reports, the total value of chips redeemed was approximately four times the total amount of chips purchased. When the dollar amount of the chips was compared to the recorded winnings in the pit area, the numbers did not correspond.

The reports also provided other evidence supporting money laundering by the defendant and associated group. Twenty-four of the CTRs recording the defendant’s transactions revealed the use of aliases and multiple Social Security numbers. On numerous other CTRs, the defendant refused to provide a Social Security number altogether.

The defendant may not have been entirely aware of the currency transaction reporting requirements in casinos. The defendant was apparently aware, however, of the currency transaction reporting requirements of banks. In addition to money laundering, the defendant was charged with structuring transactions to avoid reporting requirements. Criminals trying to hide illegal proceeds will often make a series of deposits just under the \$10,000 reporting threshold (referred to as structuring) in order to avoid having a CTR filled out recording the transaction.

In the face of the evidence against them, eight of the nine defendants in this case pleaded guilty to a 68 count superseding indictment charging distribution of marijuana, money laundering and structuring transactions to avoid reporting requirements. Criminal forfeitures in the case included millions of dollars, multiple properties, automobiles and bank accounts.

CTRs were invaluable to the success of this investigation.

(Investigating Agency: U.S. Bureau of Immigration and Customs Enforcement)

Bank Secrecy Act Records Found in Real Estate Fraud Case Lead to Separate \$1.5 Million Embezzlement Scheme

A state law enforcement agency opened an investigation against an individual for fraudulent activity related to real estate sales in Mexico. In the course of the investigation, an agent requested records filed under the BSA. Several BSA records related to the individual indicated financial activity often associated with money laundering. In fact, these records documented activity related to an embezzlement scheme at a large technology company. At the time, the alleged crime was undetected by the company or by any law enforcement authority.

The original scheme consisted of the sale of real estate in Mexico. The defendant misrepresented the value of the real estate to buyers and sellers. Many of the buyers were Americans and Canadians with no real knowledge of the true value of real estate in Mexico. The defendant would sell the properties for amounts higher than the actual sales price disclosed to the property owner/seller, keeping relevant information from the investors, and make other misrepresentations regarding the transactions. The defendant would then pocket the excess proceeds from the sales of the real estate.

To support the case, investigators contacted the state prosecutor's office for access to BSA records on the defendant, businesses controlled by the defendant, and associates of the defendant. The state prosecutor's office opened a case and found seven SARs related to the defendant and numerous CTRs. A closer examination of the SARs revealed that these records detailed an extraordinary number of checks cashed just under the \$10,000 reporting threshold.

Further investigation revealed that much of the activity took place in accounts related to a technology firm owned by the defendant. Specifically, activity occurred in accounts that regularly had deposits of checks originating from an international technology company. Investigators determined that these checks were payments for services provided by the defendant.

In fact, the defendant was working with a co-conspirator who was an employee of the technology company and who created phony invoices for services that were never performed. The defendant initially split the proceeds with the co-conspirator using checks as payment. However, recovered e-mails documented that the pair reverted to cash payments to avoid suspicion and to make transactions easier. The company was unaware of the embezzlement until notified by investigators.

Early last year, the defendant was found guilty of real estate fraud and ordered to pay restitution. The defendant is under investigation for hiding assets to prevent payment of restitution. Indictments are pending in the original embezzlement scheme.

(Investigating Agency: State Prosecutor's office)

Proactive Bank Secrecy Act Searches Lead to Crackdown on Unlicensed Money Remitters

An investigator in the District Attorney's office was conducting a proactive search in the BSA database for illicit activity and found a SAR filed on a business thought to be operating as an unlicensed money remitter. The office opened an investigation on the subjects of the SAR and obtained guilty pleas within 60 days. This investigation led to two other investigations and the eventual conviction of additional unlicensed remitters.

The case was initiated when a financial institution identified a married couple who were conducting transactions through the husband's business as indicative of the operations of a money remitter. The institution checked with FinCEN to determine if the business was registered as an MSB. When the institution did not find the business' name listed with FinCEN, it filed a SAR. A few weeks later, the District Attorney's office conducted a proactive search of SARs, located the SAR filed on one of the defendants, and opened an investigation. The investigation revealed that in a period of three years, the defendant wired millions of dollars to a foreign country through his business. Specifically, the couple made regular deposits into local banks and periodically initiated large wire transfers to the foreign country.

A few months after the SAR was filed, the District Attorney had shut down the business, arrested the couple, and moved to freeze more than \$10 million in assets.

After their arrest, the defendants cooperated with and led authorities to an associate who operated multiple businesses in state as well as offices in two other states and Canada. The associate had been in business since 1987,

and since 2000 was responsible for illicitly moving millions of dollars to the foreign country. Investigators believe that the associate controlled most of the unlicensed wire transfers to the foreign country. Like the defendants, the associate had not registered with FinCEN.

The District Attorney's office continued investigating unlicensed money remitters and soon learned of an individual operating a money remitter business out of a jewelry store. In the first eight months of 2005, that individual facilitated the movement of millions of dollars between the foreign country and the United States. Investigators believe that the individual had been in business for at least two years and used five different bank accounts to disguise the activity. The individual operated like a traditional hawala system in that not all money received was sent to the foreign country. Instead, some funds were kept to distribute to recipients of transmittal orders that had been placed in the foreign country. The individual pleaded guilty at the end of 2005 to operating an illegal money transmission business and other violations of the banking regulation.

In all three cases, the operators of the unlicensed money remitters failed to comply with state and federal laws designed to prevent money laundering. They did not check the identity of clients sending or receiving money, did not complete or file required BSA forms, nor did they screen the clients against the Office of Foreign Assets Control list of known terrorists and drug traffickers. The investigations all began with a single proactive BSA query of SARs.

(Investigating Agency: State District Attorney)

Bank Secrecy Act Records Lead to Funds for Restitution in Insurance Fraud

A series of CTRs proved crucial in identifying bank accounts used to hide proceeds obtained through insurance fraud. The fraud involved a contractor who misrepresented the number of workers in his temporary employment service. Authorities used BSA data to identify assets belonging to perpetrators.

The defendant owned and operated a company that provided temporary employees to businesses in a neighboring state. The company, which changed names a number of times in a span of five years, generally employed over 100 laborers, but only paid insurance premiums based on declarations to insurance companies that the company employed only a little more than 10 laborers.

The scheme primarily involved creating two separate companies on paper. One company would employ approximately 10 percent of the employees and

the other the remaining 90 percent. An insurance policy would be purchased only for the small company. The companies had very similar names so that they were able to mislead businesses in the neighboring state into believing the policy covered all employees of both companies. Whenever an employee was injured, the company would either arrange to pay the injured worker to avoid filing a claim, or it would file a claim in the name of the covered company. Over the course of five years, the companies were able to defraud two insurance companies of millions of dollars in premiums.

In late 2005, the defendant was sentenced in U.S. District Court for his part in the scheme to defraud insurance companies of millions of dollars. His sentence included 108 months in prison, and he was ordered to pay in excess of \$5 million in restitution to the two insurance companies.

Moreover, evidence at the defendant's trial showed that he was also engaged in an elaborate scheme to avoid paying taxes on profits from his employment service. BSA data also helped unravel this second scheme.

This scheme was accomplished by creating false business expenses and invoices from fictitious trucking companies. Money was moved from one company account to another, before converting it to currency by cashing checks at a grocery store. The defendant's company also used fictitious gasoline purchase invoices in its scheme.

The matter was turned over to the investigating arm of the state's Department of Insurance and ultimately to the U.S. Postal Inspection Service. Federal officers seized or placed under court ordered restraint numerous assets belonging to the defendant including cash, certificates of deposit, vehicles, airplanes, homes and personal assets. The total value of the assets seized approached the amount by which the insurance companies had been defrauded.

A Postal investigator said that by searching BSA information the Postal Service was able to identify two large bank accounts with a total balance of over half a million dollars. He also stated that these two accounts were the largest found belonging to the defendant. Authorities seized the funds in the accounts and designated it for restitution to the insurance companies.

(Investigating Agency: U.S. Postal Inspection Service)

Suspicious Activity Reports Help Unravel Complex Fraudulent Banking Scheme

Information from SARs helped unravel a complex fraudulent banking scheme in which victims lost thousands of dollars to fake investments and a multinational financial institution had its identity stolen.

The scheme to defraud investors allegedly started in late 2002 when an individual devised a plan to gain money from prospective investors by posing as an executive and owner of a bank on the West Coast who was about to purchase a small legitimate state-chartered, Federal Deposit Insurance Corporation-insured bank. The subject falsified official documents to support the claim. The subject also counterfeited documents that would indicate to an investor an established banking relationship with a multinational bank. In essence, the subject stole the identity of the legitimate bank.

The subject would ask prospective investors to wire money to the subject's bank. In return, the subject promised to issue certificates of deposit to show that the investments were secure. The subject obtained promises for investments of over several million dollars in the subject's so-called bank. The subject targeted very sophisticated investors and certificate of deposit brokers, and victims included a municipal government and a large credit union. Apparently, the low rate of return on the certificates of deposit was within reasonable market rates and did not immediately raise any red flags with the investors.

However, soon after investors wired over half a million dollars to the subject's account, one of the investors became suspicious and notified the FBI. Other investors, including the multinational bank, also became suspicious of the bank and its backers, and began conducting investigations. Because of the numerous inquiries, the multinational bank became aware of the false documents and filed SARs on the subject. The multinational bank received several complaints from the defrauded investors, suggesting the multinational bank had defrauded the investors when, in fact, it was itself a victim of the fraudulent scheme.

The FBI opened an investigation of the subject and retrieved BSA documents related to him, including SARs and CTRs. The SARs revealed the complexity of the case by describing forged documents and falsified bank guarantees. While the agents were aware of the subject's scheme to defraud investors, they were unaware of the threat posed to the banking system caused when the subject assumed the identity of a bank. Information in

the SARs eventually caused prosecutors to call on the affected bank's BSA compliance officer to testify at the trial on the events that caused the bank to file the reports.

It was discovered that during the scheme, the subject spent nearly \$100,000 for a lawyer, broker, and other expenses. Prosecutors stated that they believed the subject was going to use nearly \$1,000,000 of the illicitly-gained funds for the cash purchase of a home. The victims of this scheme included a church for which the defendant had promised to help secure financing for a project. The defendant also is associated with an Internet business that appears to be a pyramid scheme. Several victims have been identified and state officials are continuing to investigate this get-rich-quick scheme.

The subject was arrested and eventually convicted on 12 counts of wire fraud. The subject was released on bond pending sentencing. However, this did not hinder the subject's criminal activity. While free on bail awaiting trial, the subject lived an extravagant lifestyle beyond the subject's means and allegedly engaged in fraudulent activities and identity theft.

The government moved to revoke bond on probable cause of these additional crimes. The subject was arrested again and sentenced to five years in prison and ordered to pay nearly \$100,000 in restitution to the victims.

(Investigating Agency: Federal Bureau of Investigation)

Bank Secrecy Act Records Link Gambling Ring to Structuring at Casinos

Arrests of more than two dozen people associated with an organized crime-controlled sports-betting ring was made possible, in part, because law enforcement officials were able to track some of the subjects' suspicious financial transactions through review of BSA data. According to police, the ring handled several million dollars a month and its operators paid "tributes" to organized crime figures.

These arrests, including several organized crime associates who directed the operations and had previous gambling arrests, are part of a series of crackdowns on sports-betting rings with links to established organized crime groups. When patrons lose bets in sports betting, they have to pay immediately or face substantial interest rates on future payments, a practice that amounts to loan sharking.

One of the arrested subjects had previously attracted the attention of investigators due to a history of large cash transactions at casinos. In fact, two casinos filed SARs documenting structuring of some of those

transactions. In a period of approximately four years, the subject had been responsible for an estimated 80 casino transactions that generated CTRs totaling millions of dollars. Many of these transactions indicate money coming from the casino, and investigators are examining these transactions to determine their relationship, if any, to the sports-betting ring.

Two of the suspects' transactions caused SARs to be filed three months apart by casinos in separate states. Both SARs indicated that the subject tried to exchange chips for money in an attempt to avoid currency reporting requirements. One casino noted in the narrative that the action was highly unusual because the subject was a known customer whose activities had previously required the filing of CTRs by a casino. The other casino thought the subject's conduct was so extraordinary that in addition to filing a SAR, they sent a letter to the subject barring the subject from the casino.

Other BSA records filed on the subject include several bank CTRs, a Currency and Monetary Instruments Report, and a Form 8300 that reported a transaction in currency aggregating over \$10,000. The suspect is being investigated because the suspect is not believed by law enforcement to be in a position to have the amounts of money reported in BSA filings.

(Investigating Agency: State Police)

Bank Secrecy Act Records “Extremely Helpful” in Tracing Proceeds from Fraudulent Venture Capital Scheme

In late 2005, two individuals pleaded guilty to running a scheme to defraud hundreds of investors out of millions of dollars through phony pre-initial public offering stock sales. The pair claimed they worked for a venture capital firm that was underwriting a public stock offering for a company. In reality, the defendants used investors' money to support a lavish lifestyle. Investigators used BSA records to sift through a maze of shell companies to identify the movement of ill-gotten proceeds.

The individuals pleaded guilty to one count of securities fraud and one count of conspiracy to commit mail, wire and securities fraud, and were sentenced a few months later. Both face a maximum term of imprisonment of ten years and a maximum fine of twice the value of the loss to the victims in this matter.

Both admitted that, over a three-year span, they participated in a conspiracy to defraud investors by selling them bogus stock in a company that did not exist.

Specifically, the pair admitted to falsely representing to investors that they worked for a venture capital firm and the money the victims had invested would be used to purchase securities in what was described as a management

company. Both admitted in court that these representations were not true, and that the stock was fraudulent. After receiving the investors' funds, members of the conspiracy provided investors with bogus statements and falsely indicated that the investments would generate significant earnings. The defendants acknowledged that they did not place investors' money into investments as represented, but instead diverted the investors' funds for their own personal use and benefit and converted large amounts of the funds into cash. This scheme defrauded investors from around the country of well over \$2 million.

In an example of the reach of this fraud, a state insurance commissioner issued a cease and desist order against one of the individuals and the individual's investment company. The order details how an investor purchased approximately \$50,000 in stock through the subject. Fraudulent statements sent to the investor reported the principal as having increased by approximately 25 percent. Rather than returning the investment to the investor along with the promised earnings, the subject allegedly reinvested the money into a stock buyout that was supposed to earn the investor more than \$1,000,000. The investor never heard from the subject or anyone from the company again.

More than 80 BSA records document financial activity associated with the scheme. A senior attorney with the Securities and Exchange Commission said that:

“The CTR and SARs reports were extremely helpful in the case. As the perpetrators used false identities, operated in unknown locations, and even when properly identified posed substantial flight risks, we could not directly contact them to ask for bank and brokerage account information. Thus, the FinCEN reports were key in determining the various accounts the perpetrators controlled, as well as the general geographic area in which they operated and the names of affiliated entities. This information helped us to eventually pinpoint the perpetrators' true identities and determine the extent of their assets.”

The Securities and Exchange Commission accessed BSA records through FinCEN's Gateway program. The District Attorney's Office also supported the investigation. Other agencies involved include the FBI, Social Security Administration Office of Inspector General, United States Postal Inspection Service, and Immigration and Customs Enforcement.

(Investigating Agency: Securities and Exchange Commission)

Bank Secrecy Act Records Help Initiate Case and Lead to Networking of Separate Investigations

In 2005, a U.S. Attorney announced the indictment of three individuals operating an under-the-table payroll scheme. Under the scheme, defendants allegedly paid hundreds of temporary employees tens of millions of dollars in unreported cash payroll over a ten-year period. The case, initiated and expanded through BSA records, includes over \$15 million documented in CTRs and SARs. In addition, the indicted individuals have ties to organized crime groups.

The state police began the case through proactive searches of the BSA database. Specifically, the state police examined CTRs filed on state residents by a casino in a neighboring state. Among the more suspicious records were several filed on citizens of an aging industrial city with few viable economic opportunities. The subjects of these records were associated with temporary labor services.

As the investigation progressed, the state police learned that the three indicted individuals operated a series of labor services through straw owners and shell corporations. They would contract with businesses to provide temporary labor in a variety of industries. The businesses would pay the primary defendant by check with the understanding that the defendant was responsible for paying unemployment, Social Security, workers compensation, and other payroll taxes.

The defendant paid employees in currency and attempted to cash the checks from businesses surreptitiously. The defendant used several banks and traveled over 50 miles to use a check casher in a further attempt to hide the defendant's transactions. While at the check casher, the defendant used a private room to conduct business. However, the check casher and banks used by the defendant filed CTRs and, when appropriate, SARs. In total, the defendant's transactions resulted in the filing of 550 CTRs and 112 SARs.

The FBI became involved when an analyst reviewing SARs referred one of the subjects to an agent working on health care fraud cases. The agent, unfamiliar with the subjects, showed the SAR to the FBI's Asian organized crime group. While the group members did not recognize any of the subjects on the SAR, they did notice that the address matched a known organized crime address.

When the FBI became aware of the state police's investigation, the two joined forces with the Internal Revenue Service's Criminal Investigation Division, the U.S. Postal Inspection Service, and the state's Insurance Fraud Bureau

for additional resources and support. Investigators determined that the defendant's scheme was indeed sanctioned, supported, and protected through Asian organized crime groups. In addition, the unprecedented cooperation in the case among the participants led to the development of new investigative leads and intelligence avenues.

(Investigating Agency: State Police and the Federal Bureau of Investigation)

Suspicious Activity Report Leads to Structuring Conviction and Links to Drug Investigation

In 2005, a federal judge sentenced an individual to two years in prison for structuring monetary transactions to avoid reporting requirements. The case started when a financial institution documented unusual financial activity on a series of SARs and notified the Internal Revenue Service, which promptly opened an investigation. Meanwhile, two other federal agencies were investigating the defendant's involvement in a drug smuggling ring. The SARs helped tie the two investigations together.

In 2002, a bank filed three SARs on the defendant documenting suspicious transactions over a two-year period. These transactions consisted of regular cash deposits just under the \$10,000 reporting limit, wire transfers to offshore accounts in Canada and India, and the purchase of official checks. The activity recorded on the SARs totaled nearly \$1 million. In addition to filing the SARs, the bank also notified an Internal Revenue Service special agent of the unusual transactions. The agent had established a relationship with the bank based on a previous investigation of the defendant.

The investigation eventually led to the indictment and arrest of the defendant and the defendant's spouse on the structuring charges. While that case was unfolding, Bureau of Immigration and Customs Enforcement and Drug Enforcement Administration investigators were looking at the defendant and some associates on suspicion of drug trafficking and money laundering. Allegedly, the associates were importing precursor chemicals into the United States from Canada, and investigators believed the defendant was laundering the profits. As part of the investigation, the two agencies reviewed BSA records to help identify assets, accounts, and financial activity associated with the drug smuggling.

The BSA records retrieved included a SAR detailing the defendant's structuring and the link to the Internal Revenue Service agent leading that investigation. The three agencies joined forces to further the investigation, participate in the arrest of the subjects, and execute a search warrant in support of the indictment.

The defendant was indicted, entered into a plea agreement, and was sentenced.

(Investigating Agency: Drug Enforcement Administration)

(Intentionally left blank)

Section 4 – Tips on SAR Form Preparation & Filing

Suspicious Activity Report Form Completion Tips – A Trend Analysis of Frequently Asked Questions Received on FinCEN’s Regulatory Helpline

As in previous issues, FinCEN has reviewed recent calls received on its Regulatory Helpline¹⁶ for the most frequently asked questions about suspicious activity reporting. From May to December 2005, FinCEN responded to over 882 calls from industry and government representatives requesting suspicious activity reporting guidance. An analysis of these calls and other sources revealed the need for additional guidance in the following areas:

1. Suspicious Activity Reporting for Unregistered Money Services Businesses

In April 2005, FinCEN and the federal banking agencies issued guidance to the banking industry on providing banking services to the MSB industry.¹⁷ Among other topics, the guidance clarified that depository institutions should file SARs if they become aware that an MSB is operating in violation of the registration or state licensing requirements.¹⁸ Depository institutions are reminded, however, that, as explained below, there may be legitimate reasons for an MSB to not be registered with FinCEN or licensed in certain states.

31 C.F.R. § 103.41(b)(3) grants a newly established MSB 180 days to comply with the registration requirement. Additionally, §103.41(a)(2) clarifies that a

¹⁶ FinCEN’s Regulatory Helpline can be reached at 800-949-2732.

¹⁷ <http://www.fincen.gov/guidance04262005.pdf> and <http://www.fincen.gov/fincenadv04262005.pdf>.

¹⁸ In addition to violating the FinCEN registration regulation, which can result in both civil and criminal penalties, failure to register with FinCEN is a violation of 18 U.S.C. 1960. *See U.S. v. Uddin*, No. 04-CR-80192 (E.D.Mich. April 11, 2005). Under certain circumstances, failure to obtain a required state license to operate an MSB can also result in a violation of 18 U.S.C. 1960. *See U.S. v. Velastegui*, 199 F.3d 590 (2nd Cir. 1999). Currently, the regulation requiring registration of MSBs does not apply to the U.S. Postal Service, to agencies of the United States, of any State, or of any political subdivision of a State, or to a person to the extent that the person is an issuer, seller, or redeemer of stored value. (See 31 C.F.R. § 103.41(a)).

person who provides money services solely as the agent of another registered MSB is not required to register with FinCEN.¹⁹ Similarly, certain types of MSBs in some states may not have licensing requirements.

Further, it should be reiterated that banking organizations are not expected to terminate existing accounts of MSBs based solely on the discovery that the customer is an MSB that has failed to comply with licensing and registration requirements (although continuing non-compliance by the MSB may be an indicator of heightened risk). There is no requirement in the BSA regulations that a banking organization must close an account that is the subject of a suspicious activity report. The decision to maintain or close an account should be made by a banking organization's management under standards and guidelines approved by its board of directors. However, if an account is involved in a suspicious or potentially illegal transaction, the banking organization should examine the status and history of the account thoroughly and should determine whether or not the institution is comfortable maintaining the account. If the banking organization is aware that the reported activity is under investigation, it is strongly recommended that the banking organization notify law enforcement before making any decision regarding the status of the account.

As set forth in the April 2005 Interagency Guidance,²⁰ depository institutions must conduct a reasonable inquiry into a business' registration or licensing status before they can accurately determine whether a business is unregistered or unlicensed and thus should be the subject of a SAR. It should be clarified that a bank is not required to file a SAR if it makes a business decision to close an MSB's account based solely on the level of risk, and not on the business' registration or licensing compliance or other reportable activity. As the Interagency Guidance makes clear, requesting that the business provide copies of correspondence acknowledging their registration or licensing is one reliable method of verifying that an MSB has registered with FinCEN. As clarified later in this section (see Question 2), there should be no conflict between this request and SAR confidentiality.

19 On February 3, 2006, FinCEN issued guidance entitled, "Registration and De-Registration of Money Services Businesses." That guidance can be located at http://www.fincen.gov/msbregistration_de_registration.pdf.

20 <http://www.fincen.gov/guidance04262005.pdf>.

2. Questioning Individuals about Potentially Suspicious Activity

When determining whether suspicious activity has occurred, institutions are responsible for “examining all the facts, including the background and possible purpose of the transaction.”²¹ As part of an institution’s due diligence to determine whether suspicious activity has occurred, reasonable investigation into the nature and purpose of the activity may be necessary. Institutions have expressed concern over the perceived tension between questioning a customer about potentially suspicious activity and the institution’s responsibility to maintain the confidentiality of SARs.²²

FinCEN recognizes that under certain circumstances, institutions may discreetly question a customer about the nature and purpose of a transaction without revealing their intention to file a SAR. For example, to determine whether a customer’s transactions are “designed to evade any [reporting] requirements,”²³ an institution may wish to ask a customer why he or she is making frequent cash deposits slightly below a certain reporting or recordkeeping threshold. If the customer provides an answer that reasonably satisfies the institution that the transaction is not designed to evade reporting requirements (e.g. her business has a verifiable insurance policy that covers up to \$10,000 in currency in the event of a burglary), no SAR would be required. Financial institutions are encouraged to document SAR decisions, including final decisions not to file a SAR. (See Item 5 for additional guidance on documentation of SAR decisions).

Institutions are reminded that any questioning should not risk “tipping off” the customer or otherwise disclose that a SAR is being filed. Ultimately, institutions will need to exercise discretion and judgment when determining how and when to inquire of customers about unusual activity.

3. Continued Suspicious Activity Report Filings When No Law Enforcement Action Has Been Taken

A number of institutions, particularly after filing multiple SARs on the same individual, have contacted FinCEN to verify whether law enforcement had received the SARs or if law enforcement intended to act upon the information supplied in the reports. Institutions have questioned whether or not filing of the supplemental SARs is necessary if no law enforcement action has been taken. Law enforcement uses information in SARs to conduct investigations,

²¹ See 31 C.F.R § 103.18(a)(2)(iii) and the other SAR rules.

²² Financial institutions may not disclose to the person involved in a transaction that the transaction has been, or will be, reported. See 31 C.F.R § 103.18(e).

²³ See 31 C.F.R § 103.18(a)(2)(ii) and other SAR rules.

research, and statistical analysis, and ultimately, investigative priorities and the severity of the suspicious activity reported will determine what action, if any, is warranted.

A financial institution has an obligation to report suspicious activity as prescribed by regulation if the activity continues. FinCEN previously provided the following guidance about the subject of law enforcement contact:

As noted in the June 2001 issue of *The SAR Activity Review*, “If conduct continues for which a SAR has been filed, the guidance set forth in the October 2000 *The SAR Activity Review* (Section 5 - Repeated SAR Filings on the Same Activity) should be followed even if a law enforcement agency has declined to investigate or there is knowledge that an investigation has begun. The filing of SARs on continuing suspicious activity provides useful information to law enforcement and supervisory authorities. Moreover, the information contained in a SAR that one law enforcement agency has declined to investigate may be of interest to other law enforcement agencies, as well as supervisory agencies.”²⁴

Although a series of filings may not generate immediate contact from law enforcement, the filings could still prove vital during the investigative process at a later time. FinCEN has advised financial institutions to report ongoing suspicious activity at least every 90 days.²⁵ FinCEN encourages financial institutions to contact appropriate law enforcement *directly* if the activity reported warrants prompt attention.²⁶ Additionally, financial institutions should contact the Financial Institutions Hotline²⁷ to report suspicious activity that may relate to terrorism. As noted previously, we are in the process of reviewing the 90-day rule.

4. Suspicious Activity Reporting for “Third Party Receiver of Funds” Scams

FinCEN has received several questions regarding the filing of SARs for a prevailing type of scam that usually involves a third party wiring money order or check proceeds back to business entities located overseas. This type of fraud activity, which is referred to as a “third party receiver of funds” scam,²⁸ has features that are similar to “4-1-9” or “advance fee fraud.”

24 See *The SAR Activity Review*, June 2001, Section 6.

25 See *The SAR Activity Review*, October 2000, Section 5.

26 For examples of “appropriate law enforcement” for SAR contact, please see *The SAR Activity Review*, October 2005, Section 5.

27 The Financial Institutions Hotline can be reached at 866-556-3974.

28 Individuals who would like to report a third party receiver of funds scam may file a complaint via the Internet Crime Complaint Center, which is hosted by the FBI. The website address is <http://www.ic3.gov>.

Instead of being contacted by a person claiming to be a foreign government official located in a foreign jurisdiction, individuals are usually contacted via email or via online job postings by an entity that claims to be a legitimate business seeking financial transaction assistance in the United States. The business, usually an auction operation, will claim that due to banking restrictions placed on foreign entities, it can not easily engage in financial transactions in the United States. The business will request that the U.S. citizen cash checks or money orders on its behalf and then wire most of the proceeds back to the business. An individual may be referred to a business website that looks very professional, which tricks the individual into believing the business is legitimate.

Financial institutions become aware of the scam once a customer comes to cash the monetary instruments. Callers to the Helpline report that the monetary instruments presented are in some cases obviously fake, containing glaring spelling errors or poorly created seals. In these instances, financial institutions decline to negotiate the monetary instruments and advise the customer that the instruments are counterfeit. Other times, the monetary instruments presented appear authentic and are ultimately cashed for the customer. Later, the monetary instruments are returned as non-negotiable and either the bank or the customer must take a monetary loss.

Due to the slightly different nature of the third party receiver of funds scams in relation to the “4-1-9” and “advance fee fraud” scams, financial institutions have sought clarification on whether the third party receiver of funds scams could be treated in the manner that “4-1-9” or “advance fee fraud” scams are for SAR filing purposes. In previous guidance,²⁹ FinCEN advised financial institutions that the filing of a SAR was unnecessary for “4-1-9” or “advance fee fraud” if there was no monetary loss. FinCEN advised that a financial institution should consider filing a SAR if there was a monetary loss or if the scam involved another illegal activity (such as investment fraud, counterfeiting, forgery, misuse of a U.S. government seal, etc.). Because the activities are similar, the guidance given with regard to “4-1-9” or “advance fee fraud” scams would apply to third party receiver of funds scams as well. If the counterfeit monetary instruments are received via the U.S. postal system, financial institutions and individuals may also report the receipt to the U.S. Postal Inspection Service.

²⁹ See *The SAR Activity Review*, Issue 7, August 2004.

5. How Should a Financial Institution Document its Decision Not to File a Suspicious Activity Report?

Documentation of a financial institution's decision not to file a SAR can be useful not only in the financial institution's own internal review of its SAR decision-making and reporting procedures, but also to assist internal or external auditors and examiners in their assessment of the effectiveness of the financial institution's suspicious activity monitoring and reporting system. The *Federal Financial Institutions Examination Council's BSA/Anti-Money Laundering Examination Manual (FFIEC BSA/AML Examination Manual)* states that "[t]horough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR...Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process."³⁰

Due to the variety of systems used to identify, track and report suspicious activity, as well as the fact that each suspicious activity reporting decision will be based on unique facts and circumstances, no single form of documentation is required when a financial institution makes a decision not to file.

³⁰ While the *FFIEC BSA/AML Examination Manual* is specific to the banking industry, this question and answer regarding documentation of decisions not to file a SAR applies to all financial institutions subject to the suspicious activity reporting requirements of the BSA.

Section 5 - Issues & Guidance

This section of *The SAR Activity Review* discusses current issues raised with regard to the preparation and filing of SARs. This section is intended to identify 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 SARs.

Money Services Business Registration and De-Registration

MSBs provide valuable financial services, especially to those who may not have ready access to the banking sector. The MSB industry is quite diverse, ranging from large Fortune 500 companies with global presence to small “mom-and-pop” convenience stores in ethnic neighborhoods where English may rarely be spoken. Moreover, given the types of the products and services provided and the distribution channels, some participants in this industry sector may be at greater risk for misuse by terrorist financiers, money launderers, and other criminals. Consequently, we believe that it is vital to identify and reduce the number of unregistered MSBs in order to better focus resources to encourage increased compliance with the BSA’s programmatic, recordkeeping, and reporting requirements.

With the above background in mind, we recommend that financial institutions take time to familiarize themselves with guidance we released this past February in connection with registration and de-registration of MSBs.³¹ This guidance (FIN-2006-G006) is intended to clarify BSA requirements regarding initial registration, renewal, and de-registration of MSBs.

Important elements of the guidance include the following points:

- The failure to renew registration results in removal from our registration list. As of February 3, 2006, we have started omitting from the posted MSB Registration List any entities that have not renewed their registrations by their respective renewal deadlines. If these

³¹ See 31 C.F.R. § 103.41. In some instances, one may not, in fact, be dealing with a business that is required to register as an MSB for purposes of the BSA’s implementing regulations. In these instances, there would be no need to file a SAR due to suspicions that one was dealing with an unlicensed or unregistered MSB. We address these circumstances at greater length in Section 4 – Tips on Form Preparation and Filing.

entities were required to renew their registrations and failed to do so, we will deem those businesses to be unregistered MSBs. Additionally, we indicated that failure to register (or renew registration), could lead to civil and criminal penalties for violation of BSA regulations.

- Registration is prospective. If an MSB previously failed to register as required, but has since implemented written policies and procedures such that it is no longer providing services that require registration as a MSB, it should not register for its past activity as an MSB.
- If an entity is currently registered but no longer meets the definition of an MSB, it no longer needs to be treated as an MSB customer.
- If an entity crosses the \$1,000 MSB definitional threshold on a one-time basis, that one-time action if not repeated, does not cause the entity to become an MSB.

In light of the above guidance, qualifying MSBs should be aware that there is now an even greater expectation that they will properly acquaint themselves with and comply with the registration requirement.

Initial Registration and Registration Renewal

BSA regulations require certain MSBs to register with FinCEN whether or not they are licensed as MSBs by any state or other relevant domestic jurisdiction. The applicable definition of an MSB includes each agent, agency, branch, or office within the United States doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities: (1) currency dealer or exchanger; (2) check casher; (3) issuer of traveler's checks, money orders, or stored value; (4) seller of traveler's checks, money orders, or stored value; (5) money transmitter, regardless of the amount of money transfer services offered; and (6) the U.S. Postal Service, except with respect to the sale of postage or philatelic products. A person who does not offer one or more of the financial services specified in (1) through (4) above in an amount greater than \$1,000 in currency or monetary or other instruments for any one person on any one day in one or more transactions is not covered by the definition of an MSB, and therefore is not required to register.

At the present time, the following MSBs are excepted from the registration requirement:

- A business that is an MSB *solely* because it serves as an agent of another MSB;

- A business that is an MSB *solely* as an issuer, seller, or redeemer of stored value; and
- The U.S. Postal Service and agencies of the United States, or any State, or of any political subdivision of any State.

Additionally, branch offices of an MSB are not required to file their own registration forms.

Depository institutions and persons registered with and regulated or examined by, the Securities and Exchange Commission or the Commodity Futures Trading Commission for BSA compliance that offer otherwise qualifying money services are not defined as MSBs and, therefore, are not required to register. Likewise, casinos and card clubs are not required to comply with rules specific to MSBs.

Initial registration of MSBs in existence 180 days or more before December 31, 2001 was required on or before December 31, 2001. These MSBs were then required to renew their registrations by December 31, 2003 if they continued to qualify as MSBs. Thereafter, for these entities, the requirement is to continue to renew registrations every two years (by December 31, 2005, 2007, 2009, etc.) for as long as the business continues to operate as a qualifying MSBs.

Initial registration of MSBs established after December 31, 2001 is required before or by the end of 180 days after the date of establishment as MSBs. An initial registration period begins January 1 of the year in which a business is required to register and ends December 31 of the second calendar year. These MSBs are required to renew their registrations for the first time at the end of their initial registration periods. Thereafter, registration renewal is required every two years by December 31 for as long as the entities continue to operate as qualifying MSBs.

Re-registration

Re-registration is required if there is:

- A change in the ownership or control that requires the business to re-register under state law;
- A transfer of more than 10 percent of the voting power or equity interests of the MSB (other than one that must be reported to the Securities and Exchange Commission);
- A greater than 50 percent increase in the number of agents.

The calendar year in which the ownership change, equity transfer, or agent

increase occurs is treated as the first year of a new (initial) two-calendar year registration period. Such re-registration initiates a new calculation for determining renewal deadlines, just as an initial registration period does for calculating subsequent renewal deadlines.

De-registration and Ceasing to be a Money Services Business

There is currently no provision in the BSA regulations or procedures to allow an MSB to de-register even if the business is no longer providing services that require registration as an MSB. At the present time, the only option for an entity that has ceased to operate as an MSB, or that has registered incorrectly, is to refrain from renewing its registration. If the entity does not renew its registration, after the two-year renewal deadline has passed and we determine that the business is no longer currently registered we will omit the business from the posted MSB Registration List.

The date upon which an entity implements (not merely adopts) written policies and procedures that would exclude it from the definition of MSB is the effective date upon which the business ceases to be an MSB. For example, a check casher that registered as an MSB because it cashed checks at a level that met the regulatory definition (i.e., in an amount greater than \$1,000 in currency or monetary or other instruments for any person on any day in one or more transactions), but has subsequently implemented written policies and procedures to no longer offer check cashing services that reach the \$1,000 definitional threshold for a check casher, has ceased to be an MSB. This is the case even if the business continued to cash checks, provided that it does not cash checks in an amount that triggers the definitional threshold for an MSB. (See FinCEN Ruling 2005-3.) Such a business should not renew its registration when it expires. Moreover, other entities are no longer required to continue treating an entity that has ceased to meet the definition of an MSB as an MSB customer.

For additional guidance on MSB registration requirements, please call FinCEN's Regulatory Helpline at (800) 949-2732 or visit FinCEN's website at www.msb.gov.

Grand Jury Subpoenas and Suspicious Activity Reporting

In an effort to improve the consistency and quality of information being reported in SARs, and to guide financial institutions on compliance with suspicious activity reporting requirements, FinCEN is issuing this

guidance about whether, when and how a financial institution should file a SAR after being served with a grand jury subpoena.

Grand juries issue subpoenas in furtherance of conducting investigations of subjects and targets of their proceedings, and therefore the receipt of such a subpoena does not, by itself, require the filing of a SAR.³² Nonetheless, the receipt of a grand jury subpoena should cause a financial institution to conduct a risk assessment of the subject customer and also review its account activity.³³ If suspicious activity is discovered during any such assessment and review, the financial institution should consider elevating the risk profile of the customer and filing a SAR in accordance with applicable regulations.³⁴ Unless there is something suspicious about the activities of a customer, apart from the service of the grand jury subpoena, a SAR should not be filed.

Receipt of a grand jury subpoena also does not alter the standards for filing a SAR. Financial institutions should only file a SAR for transactions conducted or attempted by, at, or through the financial institution involving or aggregating at least \$5,000 when the financial institution knows, suspects, or has reason to suspect that (1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities; (2) the transaction is designed to evade any requirements under the BSA; (3) 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 bank knows of no reasonable explanation for the transaction after examining all the available facts; or (4) the transaction involves use of the financial institution to facilitate criminal activity.³⁵

³² See note 33, *infra*.

³³ See, e.g., *In the Matter of the Federal Branch of Arab Bank PLC*, Financial Crimes Enforcement Network, Enforcement Action No. 2005-2 at fn.15 (August 17, 2005) (“while a subpoena from law enforcement does not represent, in and of itself, cause for filing a SAR, the subpoena is an important piece of information that places a financial institution on notice of the need to conduct a further review of accounts or activity involving the subject of the subpoena to identify potentially suspicious activity”).

³⁴ See 31 C.F.R. § 103.16(b)(2) (suspicious activity reporting requirements for insurance companies); 31 C.F.R. § 103.17(a)(2) (for futures commission merchants and introducing brokers in commodities); 31 C.F.R. § 103.18(a)(2) (for banks); 31 C.F.R. § 103.19(a)(2) (for brokers and dealers in securities); 31 C.F.R. § 103.20(a)(2) (for MSBs, which are required to report suspicious activity involving or aggregating funds or assets of at least \$2,000); and 31 C.F.R. § 103.21(a)(2) (for casinos).

³⁵ See *id.* FinCEN’s suspicious activity reporting requirement for banks does not contain the fourth reporting category listed above. However, banks are also subject to the suspicious activity reporting requirements of their federal functional regulators, which contain a similar reporting category. See 12 C.F.R. §§ 208.62, 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System); 12 C.F.R. Part 353 (Federal Deposit Insurance Corporation); 12 C.F.R. Part 748 (National Credit Union Administration); 12 C.F.R. § 21.11 (Office of the Comptroller of the Currency); and 12 C.F.R. § 563.180 (Office of Thrift Supervision).

The failure to adequately describe the factors making the reported transaction or activity suspicious in the narrative of a suspicious activity report lessens its usefulness to law enforcement. Therefore, if a financial institution does prepare a SAR following the service of a grand jury subpoena, it should provide detailed information about the facts and circumstances of the detected suspicious activity, rather than the mere fact that a grand jury subpoena has been received.

Finally, grand juries are confidential proceedings conducted by state and federal prosecutors to determine whether enough evidence exists to formally accuse the subjects of criminal charges. A financial institution that receives a grand jury subpoena in connection with an investigation relating to a possible crime against any financial institution or supervisory agency, or certain other crimes, is prohibited from directly or indirectly notifying any person named in the subpoena about the existence or contents of the subpoena, or information that the financial institution has furnished to the grand jury in response to the subpoena.³⁶

If a financial institution has any questions about SAR filing related to grand jury subpoenas, or about suspicious activity reporting in general, it should contact FinCEN's Regulatory Helpline at (800) 949-2732.³⁷ Financial institutions with a federal functional regulator may also wish to call that regulator with questions related to that regulator's suspicious activity reporting requirements, procedures and records the financial institution should maintain.

When Does the 30-Day Time Period in which to File a Suspicious Activity Report Begin?

Guidance on when a SAR must be filed was first set forth in the October 2000 SAR Activity Review: Tips, Trends & Issues. We are issuing updated guidance on this topic to clarify ambiguity in the interpretation of the original guidance.

³⁶ See 12 U.S.C. § 3420(b). In addition, because of the confidentiality of grand jury proceedings and the unindicted status of the subjects, financial institutions should take appropriate measures to ensure the confidentiality of grand jury subpoenas and their contents, which could include refraining from referencing in the SAR the fact that the bank received a grand jury subpoena.

³⁷ Financial institutions need not notify FinCEN of requests for SARs that are made by law enforcement pursuant to grand jury subpoenas. If a financial institution needs to notify FinCEN about a request for a SAR, the financial institution should contact FinCEN's Office of Chief Counsel directly at (703) 905-3590.

Our suspicious activity reporting rules require that a SAR be filed no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR.³⁸ If no suspect can be identified, the time period for filing a SAR is extended to 60 days. Upon identification of unusual activity, additional research is typically conducted, and institutions may need to review transaction or account activity for a customer to determine whether to file a SAR. The need to review a customer's account activity, including transactions, does not necessarily indicate the need to file a SAR, even if a reasonable review of the activity or transaction might take an extended period of time. The time period to file a SAR starts when the institution, in the course of its review or as a result of other factors, reaches the conclusion in which it knows, or has reason to suspect, that the activity or transactions under review meets one or more of the definitions of suspicious activity.³⁹

The phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an account holder's normal account activity. A real estate investment (purchase or sale), the receipt of an inheritance, or a gift, for example, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. The institution's automated account monitoring system or initial discovery of information, such as system-generated reports, may flag the transaction; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulations.

A review must be initiated promptly upon identification of unusual activity that warrants investigation. The timeframe required for completing review of the identified activity, however, may vary given the situation. According to the FFIEC's 2005 *Bank Secrecy Act/Anti-Money Laundering Examination Manual*,⁴⁰ "an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed in a reasonable period of time."⁴¹ What constitutes a "reasonable period of time" will vary according to the facts and circumstances of the particular matter being reviewed and the effectiveness

38 31 C.F.R. § 103.17; 31 C.F.R. § 103.18; 31 C.F.R. § 103.19; 31 C.F.R. § 103.20; 31 C.F.R. § 103.21

39 BSA Advisory Group, "Section 5 – Issues and Guidance" *The SAR Activity Review-Trends, Tips & Issues*, October 2000, page 27.

40 An electronic version of the *FFIEC BSA/AML Examination Manual* may be found at http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

41 While the *FFIEC BSA/AML Examination Manual* is specific to the banking industry, this piece of guidance is also applicable to other industries with suspicious activity reporting requirements.

of the SAR monitoring, reporting, and decision-making process of each institution. The key factor is that an institution has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed.

For violations requiring immediate attention, in addition to filing a SAR, financial institutions should immediately notify law enforcement via telephone, and as necessary, their functional regulator. For suspicious activity related to terrorist activity, institutions may also call FinCEN's toll-free hotline at 1-866-556-3974 (7 days a week, 24 hours a day) to further facilitate the immediate transmittal of relevant information to the appropriate authorities.

Section 6 - Industry Forum

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into some aspect of compliance management or fraud prevention that presents their view of how they implement the BSA within their institutions. 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 the U.S. Government.

Transaction Monitoring & Reporting for Money Services Businesses

By: Peter Ziverts, on behalf of the Non Bank Funds Transmitters Group

Money Services Businesses (MSBs) come in a wide variety of sizes and shapes. They range from sophisticated, publicly traded money transfer companies and check cashing chains to ‘mom and pop’ grocery stores.

They also vary in the types and scope of services they provide. Western Union, for example, is an MSB by virtue of its role as a “wholesaler” of money transfer services and money orders. Wholesale, or primary, MSBs typically do not interface directly with consumers at the point-of-sale (though they generally provide telephone customer service support). Instead, they provide their financial services and systems to retailers – also MSBs – which sell them to the end user. Retail MSBs serve as the direct consumer interface and vary widely within their category, ranging from independent ‘mom and pop’ locations to national grocery chains.

What these businesses have in common is that they all offer a host of much-needed financial services to individuals – both with and without banking relationships – and businesses. And, as financial institutions, they also have a common responsibility under the BSA to implement and maintain an effective anti-money laundering compliance program that is reasonably designed to prevent itself from being used to facilitate money laundering or the financing of terrorism. Clearly, transaction monitoring and reporting – both SARs and CTRs – are vital components of this responsibility.

It is through their transaction monitoring and reporting responsibilities that these vastly different types of businesses have a critical nexus in protecting our nation's financial system from potential abuse. Viewing individual and aggregate transaction activity through different lenses serves as the basis for filing meaningful reports, which provide valuable assistance in law enforcement investigations.

Transaction Monitoring: A Dual View

MSBs identify and report suspicious activity to the IRS on a SAR-MSB form. Much like banks, a SAR-MSB must be filed if an MSB knows, suspects, or has reason to suspect that a transaction or series of transactions involves money laundering, violation of the BSA (including structuring), terrorist financing, other violation of criminal law, or serves no apparent lawful purpose.

Primary MSBs and their agents each have a responsibility to monitor and report suspicious activity, which they do on two levels: 1) subjectively, at the agent MSB level through direct consumer contact and 2) at the primary MSB level through objective, data driven analysis.

At the agent level, employees are trained to identify suspicious activity by monitoring consumer behavior, such as:

- Hurried, nervous or evasive consumers
- Consumers who know too much about BSA reporting and recordkeeping rules
- A consumer who is aggressive or uncooperative
- Someone who is reluctant to provide ID when requested
- Someone who provides inconsistent information when asked questions
- Consumers who conduct multiple transactions just below reporting or recordkeeping thresholds
- A consumer who offers a bribe or "tip" to bend the rules
- ID documents that appear to have been altered or forged
- Multiple consumers who approach the store together, but ignore each other and conduct separate transactions once inside
- Different consumers sending funds to the same person

Agent MSBs file SARs based on subjective consumer behavior and transaction activity, and they can support this view through software provided by the primary MSB. For example, Western Union provides its agents with software that allows them to monitor their transaction activity on an aggregated basis, looking for additional suspicious activity by examining principal, volume and frequency patterns, among other clues.

Such tools provide several options. An agent's Compliance Officer can identify suspicious activity by reviewing raw transaction data alone. Another option is the creation of *internal* suspicious transaction reports, which, after several days or a week, a Compliance Officer can review alongside general transaction activity, and copies of consumer forms and receipts, to identify potential suspicious activity and file SARs accordingly.

The key to successful agent level suspicious activity reporting is: 1) employee training and 2) regular review. Primary MSBs should have tools to facilitate and encourage a robust agent suspicious activity review and reporting process. Such support can be provided through analytical software, agent training assistance and periodic review of the agent's internal procedures.

In contrast to an agent's localized view, primary MSBs have a view of their entire network and can objectively analyze aggregated transaction data to identify, for example, basic structuring or smurfing activity, as well as more nuanced activity such as one person sending funds to multiple jurisdictions, many senders concentrating funds to one recipient or linked transaction patterns.

Because monitoring is one of the most effective ways for a primary MSB to "know its customers" they should have sophisticated analytical software that can identify transactional "red flags", i.e. structuring, as well as allow for customized research. Most monitoring systems review single day activity as well as activity over longer periods of time to allow for the identification of patterns. Taking this longer term look will provide law enforcement with more meaningful reports.

And the world is a big place – especially when it comes to keeping track of millions of transactions. Even though suspicious activity reporting is required in only a handful of countries, an MSB's systems should not only be capable of reviewing U.S.-centric activity, but also allow for the monitoring of offshore activity, particularly in higher risk jurisdictions.

This dual, or holistic, view to transaction monitoring provides a comprehensive system for understanding consumer activity and identifying suspicious activity, which serves as the backbone for meaningful reporting.

Assessment & Control: It's All About Risk

Having an effective view over transaction activity serves as a *gateway* to filing meaningful reports. Once inside the gate, it takes thoughtful transaction analysis to: 1) know what activities and patterns to look for and 2) understand and determine what information will be useful to law enforcement in a SAR filing. Thorough analysis depends on robust systems for risk assessment and control, which lie at the heart of a robust MSB anti-money laundering compliance program.

Based on the nature of the MSB, risk profiles incorporate many factors. Primary MSBs consider such factors as:

Products

What is the purpose of each product and what is its inherent risk - that is, the level of risk before the application of controls, systems, and processes used to reduce the risk?

For example, on a given risk continuum, money orders – because of their potential for anonymity – are generally considered riskier than consumer-to-consumer money transfers, which require a certain level of sender and receiver information. On the same continuum, consumer-to-consumer money transfers are generally considered riskier than consumer-to-business money transfers because the primary MSB has an ongoing subscriber relationship with the receiving entity – on which it has conducted due diligence – and collects certain information from the sender. The increasing popularity of prepaid debit cards – which can have some similarity to money orders – are giving rise to new risk considerations and questions.

Sender/Receiver Relationship

The relationship between the sender and the receiver offers another risk touch point: consumer-to-consumer, consumer-to-business, business-to-consumer and business-to-business. Each of these carry different risk profiles based on the relationships each has to the other and the relationship each has with the primary MSB.

Geography

Agent locations and transactions taking place in High Intensity Financial Crime Areas (HIFCAs) and High Intensity Drug Trafficking Areas (HIDTAs) also affect risk, although the HIFCA and HIDTA designations have become

so general that their practicality is questionable. Better yet is review and analysis of money transfer corridors, which can provide deeper insight into questionable activity.

Agents

Agents also play a role in risk assessment because large agents – national or regional chains – will have a greater degree of anti-money laundering compliance sophistication and more resources than the small ‘mom & pop’ agents. This consideration plays a significant role in the frequency and depth of agent anti-money laundering program reviews by primary MSBs, and the banks that provide their banking services. The inherent risk of agents with high transaction volumes is mitigated by more frequent program reviews. And, certain agents – perhaps those in former Non-Cooperative Countries and Territories – warrant consistent monitoring and transaction analysis.

Rating Risks

Alas, all risks are not created equal. Individual risks should be rated using a risk rating methodology, which can be a complex task. Risk rating systems can look any one of the following ways – or more:

- High – Medium – Low
- Extremely High – Moderate High – Medium – Moderately Low – Extremely Low
- Number rating 1-5 or 1-10
- Acceptable – Unacceptable

Applying such systems depends on defining each risk rating and identifying which characteristics qualify as high, medium or low. Criteria for defining the ratings can vary by business and the type of service being provided.

For one business, High Risk might mean the regulatory requirement is complex, carries potentially large fines, has changed recently and no updated controls are in place, no training has been done, and the monitoring process used is entirely manual.

On the other hand, Low Risk could still mean the existence of complex regulatory requirements and fines, but the product has an inherently lower risk consumer-to-business business model, supported by robust monitoring and control systems and extensive agent training.

All of the factors can vary based on an MSB's anti-money laundering sophistication, systems/automated monitoring capability and management commitment to anti-money laundering compliance.

At The End Of The Day ... It's About The People

Computers, software and risk assessment are just the foundation of an effective monitoring program. The real 'Intelligence' comes from the analyst. While a computer may flag activity for review, it is the person looking at the screen who should determine whether a series of transactions is a reportable event.

Therefore, analysts should be highly trained and motivated. They should fully understand the MSB's business model, its customer base and cultural diversity, as well as the BSA and typical money laundering schemes. This knowledge set can be gained through formal seminars, in-house training/onboarding and on-the-job mentoring and coaching. New analysts can start by reviewing large currency transactions and graduate to standard SAR reviews. However, customized reviews and those encompassing higher risk jurisdictions should be handled by senior-level analysts, preferably ones familiar with the geopolitical and cultural characteristics of the areas in question. Such senior level analysts can also act as liaisons to law enforcement, thereby increasing their own understanding of what to look for and how to better report it.

Finally, an effective risk-based monitoring program will collect intelligence from every possible source, above and beyond mere transaction data. Law enforcement contacts are essential to addressing potential risk and knowing where to point the telescope. Continued dialogue with the MSB's business people, sales staff and agent base can provide early warnings to anomalies later detected in the system.

By thoroughly understanding the risks associated with various consumers, services and geographies, MSBs can develop an effective suspicious review mechanism. This mechanism – part machine, part human and driven fully by management's unwavering commitment to anti-money laundering compliance – can help ensure that MSBs can address and mitigate risks effectively as we as provide law enforcement with meaningful information to protect our nation's financial system.



Section 7 - Feedback Form

Financial Crimes Enforcement Network U.S. 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. This form can also be accessed and completed online by visiting <http://www.fincen.gov/feedback/fb.sar.artti.php>. Any questions can be submitted to sar.review@fincen.gov.

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 Operator

Money Services Business:

- Money Transmitter
- Money Order Company or Agent
- Traveler's Check Company or Agent
- Currency Dealer or Exchanger
- U.S. Postal Service

Casino or Card Club

- Casino located in Nevada
- Casino located outside of Nevada
- Card Club

Other (please identify): _____

B. Please indicate your level of satisfaction with each section of this issue of *The SAR Activity Review- Trends Tips and Issues* (circle your response).

1=Not Useful, 5=Very Useful

Section 1 - Director's Forum	1	2	3	4	5
Section 2 - Trends and Analysis	1	2	3	4	5
Section 3 - Law Enforcement Cases	1	2	3	4	5
Section 4 - Tips on SAR Form Preparation & Filing	1	2	3	4	5
Section 5 - Issues & Guidance	1	2	3	4	5
Section 6 - Industry Forum	1	2	3	4	5
Section 7 - Feedback Form	1	2	3	4	5

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

(Intentionally left blank)

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

E. Did you find the Index listing of previous and current SAR Topics useful?

Yes

No

F. What new TOPICS, 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.

G. What questions does your financial institution have about *The SAR Activity Review* that need to be answered?

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

- October 2000 June 2001 October 2001 August 2002
 February 2003 November 2003 August 2004 April 2005
 October 2005

Please fax Feedback Forms to:

**Financial Crimes Enforcement Network (FinCEN)
(202) 354-6411**

Appendix

Index of Topics from previous issues of The SAR Activity Review

Topic	Issue	Page	Hyperlink Address to <i>SAR Activity Review</i> 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
Casino and Card Club Industries – Suspicious Activity Report Filings	8	19	http://www.fincen.gov/sarreviewissue8.pdf
Computer Intrusion	3	15	http://www.fincen.gov/sarreviewissue3.pdf
Computer Intrusion	9	15	http://www.fincen.gov/sarreviewissue9.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
Detection of Unlicensed/Unregistered MSBs through SAR Filings	10	5	http://www.fincen.gov/sarreviewissue10.pdf
Director’s Forum: Issue 8	8	3	http://www.fincen.gov/sarreviewissue8.pdf
Director’s Forum: Issue 9	9	3	http://www.fincen.gov/sarreviewissue9.pdf
Director’s Forum: Issue 10	10	3	http://www.fincen.gov/sarreviewissue10.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: BSA Compliance by the MSB Industry	10	47	http://www.fincen.gov/sarreviewissue10.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
Industry Forum: An Overview of Suspicious Activity Report Training Elements in 2005	8	43	http://www.fincen.gov/sarreviewissue8.pdf
Industry Forum: USA PATRIOT Act's Full Weight Placed on Securities Firms	9	47	http://www.fincen.gov/sarreviewissue9.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: Grand Jury Subpoenas and SARs	10	42	http://www.fincen.gov/sarreviewissue10.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: MSB Registration and De-Registration	10	39	http://www.fincen.gov/sarreviewissue10.pdf
Issues and Guidance: National Security Letters and Suspicious Activity Reporting	8	35	http://www.fincen.gov/sarreviewissue8.pdf
Issues and Guidance: Office of Foreign Assets Control (OFAC)	4	49	http://www.fincen.gov/sarreview082002.pdf
Issues and Guidance: Office of Foreign Assets Control's List of Specially Designated Nationals and Blocked Persons- Revised Guidance on filing Suspicious Activity Reports	8	38	http://www.fincen.gov/sarreviewissue8.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: Providing SARs to Appropriate Law Enforcement	9	43	http://www.fincen.gov/sarreviewissue9.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: Suspicious Activity Involving the Iraqi Dinar	8	41	http://www.fincen.gov/sarreviewissue8.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
Issues and Guidance: When does the 30-day Time Period for Filing SARs Begin?	10	44	http://www.fincen.gov/sarreviewissue10.pdf
Law Enforcement Case: 314(a) Results Enhance Material Support for Terrorism Case	7	30	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Attorney and Three Accomplices Convicted in Multi-Million Dollar Real Estate Fraud	7	35	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 Integral to FBI Information Mapping Technology	10	17	http://www.fincen.gov/sarreviewissue10.pdf
Law Enforcement Case: BSA Data Leads to \$18 Million Seizure	7	31	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Charity Evades Reporting Requirement	8	26	http://www.fincen.gov/sarreviewissue8.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	35	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: Fraudulent Banking and Investment Scheme, Identity Theft	10	25	http://www.fincen.gov/sarreviewissue10.pdf
Law Enforcement Case: Fraudulent Venture Capital Scheme	10	27	http://www.fincen.gov/sarreviewissue10.pdf
Law Enforcement Case: Hawala Investigation	6	38	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Hawala Operation	8	26	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Identity Theft	9	34	http://www.fincen.gov/sarreviewissue9.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: Insider Fraud Contributes to Bank Failure	8	28	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Insurance Executive Embezzled from Local Government's Self-Insured Health Fund	7	36	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Insurance Fraud	10	23	http://www.fincen.gov/sarreviewissue10.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: Loan Officer Fraud at Depository Institution	9	33	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Marijuana Farm Owner Sentenced	8	27	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Mail Fraud and Structuring by Attorney	9	36	http://www.fincen.gov/sarreviewissue9.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: Methamphetamine Production Ring	3	31	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Misapplication of Funds at Depository Institution	9	33	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Money Laundering and Pyramid Scheme	8	28	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Money Laundering by Drug Traffickers through Casinos	10	20	http://www.fincen.gov/sarreviewissue10.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 Laundering through Imported Edible Delicacies	9	34	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Money Laundering through Wire Transfers to South American Countries	9	37	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Money Remitter Sending Money to Iraq	5	52	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Money Remitting Business Laundering Drug Proceeds	8	28	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Nigerian Advance Fee Scam	6	40	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Nigerian Round-Tripping Investigation	7	32	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Non-Profit Organization Operating as Money Remitter	7	31	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Operation Cheque Mate	9	31	http://www.fincen.gov/sarreviewissue9.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: Payroll Scheme with ties to Organized Crims	10	23	http://www.fincen.gov/sarreviewissue10.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: Ponzi Scheme	10	19	http://www.fincen.gov/sarreviewissue10.pdf
Law Enforcement Case: Real Estate Fraud and Embezzlement	10	21	http://www.fincen.gov/sarreviewissue10.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: Structured Deposits Exceeding \$700,000	7	34	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Structuring and Food Stamp Fraud	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Structuring and Money Laundering related to Drug Investigation	10	30	http://www.fincen.gov/sarreviewissue10.pdf
Law Enforcement Case: Structuring and Tax Evasion	9	35	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Structuring and Tax Evasion by Service Company Owner	9	36	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Structuring by Three Family Members	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Structuring at Casinos by Organized Crime	10	20	http://www.fincen.gov/sarreviewissue10.pdf
Law Enforcement Case: Tax Evasion Case	4	38	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Tax Evasion Case	9	35	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Tax Evasion by a Business Owner	8	27	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Telemarketing Fraud	7	33	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Terrorism Investigation	8	25	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Travel Agent	2	29	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Unlicensed Money Remitter	10	22	http://www.fincen.gov/sarreviewissue10.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
Mortgage Loan Fraud Trends	10	13	http://www.fincen.gov/sarreviewissue10.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: Continued SAR Filings When No Law Enforcement Action Has Been Taken	10	35	http://www.fincen.gov/sarreviewissue10.pdf
SAR Tips: Definitions and Criminal Statutes for SAR Characterizations of Suspicious Activity	7	39	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Documenting Decisions Not To File SARs	10	38	http://www.fincen.gov/sarreviewissue10.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: Frequently Asked Questions Received on FinCEN’s Regulatory Helpline	8	29	http://www.fincen.gov/sarreviewissue8.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: Insignificant SAR Filing Errors	9	42	http://www.fincen.gov/sarreviewissue9.pdf

SAR Tips: Instructions for Completing the SAR Form	6	50	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: Problems with Taxpayer Identification Numbers	9	39	http://www.fincen.gov/sarreviewissue9.pdf
SAR Tips: Questioning Individuals about Potentially Suspicious Activity	10	35	http://www.fincen.gov/sarreviewissue10.pdf
SAR Tips: SAR Filing Tips for MSBs	4	42	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: Suspicious Activity Reporting for Unregistered MSBs	10	33	http://www.fincen.gov/sarreviewissue10.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: Suspicious Activity Reporting for Third Party Received of Funds Scams	10	36	http://www.fincen.gov/sarreviewissue10.pdf
SAR Tips: Special Guidance Related to Identity Theft and Pretext Calling	2	34	http://www.fincen.gov/sarreview2issue4web.pdf
SAR Tips: Suspicious Activity at a Location Other than the Institution	9	40	http://www.fincen.gov/sarreviewissue9.pdf
SAR Tips: Suspicious Activity Reporting Guidance for Casinos	7	37	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Suspicious Activity without a Loss to the Institution	9	41	http://www.fincen.gov/sarreviewissue9.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
Securities and Futures Industries – SAR Analysis	9	5	http://www.fincen.gov/sarreviewissue9.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
Terrorist Financing Suspicious Activity Reports	8	5	http://www.fincen.gov/sarreviewissue8.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