



Issue 12
October 2007

The SAR Activity Review Trends, Tips & Issues

The SAR Activity Review

Trends
Tips &
Issues

Issue 12

Published under the auspices of the BSA Advisory Group.

Table of Contents

Introduction	1
Section 1 – Director’s Forum.....	3
Section 2 – Trends & Analysis.....	5
Trends in Suspicious Activity Reports Involving Convenience Checks.....	5
Use of the Category “Other” on Suspicious Activity Reports.....	12
Credit Union Cooperatives.....	15
Section 3 – Law Enforcement Cases.....	21
Investigations Assisted by Bank Secrecy Act Data.....	21
Section 4 – Issues & Guidance.....	33
Definitions and Criminal Statutes	33
Section 5 – Industry Forum	37
Suspicious Activity Reporting Issues Confronting the Money Services Business Industry	37
Section 6 – Feedback Form	41
Appendix –	45
Index of Topics from All Editions of The SAR Activity Review – Tends, Tips & Issues	45

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.

We are continuing to provide expanded descriptions of law enforcement cases included in Section 3 to better demonstrate how important and valuable Bank Secrecy Act (BSA) data is to the law enforcement community. Many of these cases, which range in topic from high-yield investment schemes to international money laundering, 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 addresses several noteworthy topics. The articles include perspectives on the BSA as it affects convenience checks and credit card cooperatives, including analytical reviews. An industry viewpoint addresses SAR reporting issues confronting the money services business industry. Finally, this issue contains guidance on definitions and criminal statutes for the SAR characterizations of suspicious activity.

The SAR Activity Review is possible only as a result of the extraordinary work of many FinCEN employees and FinCEN’s regulatory, law enforcement and industry partners. In order to recognize that hard work, we acknowledge contributors throughout the Review.

Below is a summary of topics addressed in this issue.

- Section 1: Director’s Forum;
- Section 2: Trends and Analysis – Trends in Suspicious Activity Reports Involving Convenience Checks; Use of the Category “*Other*” on Suspicious Activity Reports; and Findings from Suspicious Activity Reports Referencing Credit Union Cooperatives;

¹ Participants include, among others, the American Bankers Association; Independent Community Bankers of America; American Institute of Certified Public Accountants; Securities and Financial Markets 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. Securities and Exchange Commission; U.S. Department of Justice’s Criminal Division and Asset Forfeiture & Money Laundering Section and the Federal Bureau of Investigation; Drug Enforcement Administration; 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 3: Law Enforcement Cases – Investigations Assisted by Bank Secrecy Act Data;
- Section 4: Issues and Guidance – Definitions and Criminal Statutes for the Suspicious Activity Report Characterizations of Suspicious Activity;
- Section 5: Industry Forum – Suspicious Activity Reporting Issues Confronting the Money Services Business Industry; and
- Section 6: Feedback Form.

Your comments and feedback are important to us. Please take a moment to let us know if the topics chosen are helpful. To help you submit your comments, we have included a feedback form in Section 6.

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

Robert Rowe
Regulatory Counsel
Independent Community Bankers of America
1615 L Street, NW
Suite 900
Washington, DC 20036-5623
P: 202-659-8111
F: 202-659-9216
robert.rowe@icba.org
www.icba.org

Rebecca Lassman
Senior Advisor
Financial Crimes Enforcement
Network (FinCEN)
(202) 354- 6400 (phone)
Rebecca.Lassman@fincen.gov or
sar.review@fincen.gov

Section 1 – Director’s Forum



*James H. Freis, Jr.
Director, FinCEN*

It is again my pleasure to present *The SAR Activity Review*. This twelfth edition brings several informative articles and many more examples of how law enforcement agencies are using the information that you provide to discover and disrupt criminal enterprises and protect the financial system. The information collected through Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and the other forms required by the Bank Secrecy Act (BSA) is used *every day* by authorized law enforcement professionals, FinCEN, and other regulators. Once again, I am pleased to share with you examples of the value that BSA information brings to investigations, criminal cases, and regulatory analysis.

Since the last Review, FinCEN, with the support of Treasury Secretary Henry M. Paulson, Jr, has launched a series of initiatives to make the administration of the BSA more efficient for those in industry covered by its requirements and more effective for those in the law enforcement and regulatory communities who rely on this information. Secretary Paulson announced initiatives that support FinCEN’s taking a fresh look at matching risk-based examinations to risk-based obligations, examining issues surrounding Money Services Businesses (MSBs), looking at ways to make FinCEN’s regulations more intuitive, and enhancing feedback from FinCEN, and other government agencies to the various sectors of the financial industry. (A broader discussion of these topics can be found on the new *BSA Regulatory Effectiveness and Efficiency* section of our website.) Of these several initiatives, one is particularly relevant to this publication: *Feedback*.

FinCEN continues to devote significant effort and seize appropriate opportunities to enhance communication with the industries it covers to promote a common understanding of the important role that BSA information plays in protecting the financial system. The American people, through their Congress, made the public-policy decision to rely on financial institutions to provide important information concerning suspicious activities and certain financial events and transactions. FinCEN, law enforcement, other regulators, and these financial institutions are partners in this effort. No one is in a better position than those in the industry to see and understand individual transactions. FinCEN has the privilege to collect, analyze and store this valuable information both for its own use and for the

benefit of other agencies for analysis and investigation. Everyone involved in this partnership has an interest in both giving and receiving quality feedback to and from the other partners.

This *Review* is but one of the many ways that FinCEN demonstrates its commitment to providing feedback to the industry. The companion publication, *The SAR Activity Review, By the Numbers*, also provides useful raw data on the types and quantity of BSA reports that are being filed. The BSA Advisory Group provides a forum for the industry, regulators, and law enforcement professionals to share issues of mutual concern. FinCEN's Office of Outreach Resources provides support to financial institutions through developing guidance, training, and education. On an almost weekly basis FinCEN provides expert speakers and panelists for a range of national, and sometimes international, industry conferences. With the help of U.S. Treasurer Anna Cabral, FinCEN recently announced and published informative MSB brochures in seven different languages including; Spanish, Farsi, Chinese, Russian, Arabic, Vietnamese and Korean. Another useful reference document, *Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting*, was recently made available on our website. FinCEN's website itself will soon be renovated to allow for easier use and access to information. That process involves surveying and interviewing leaders in the industry, media, regulatory, and law enforcement communities to make sure we hear what you would like to see.

Personally, my schedule is filled with meetings and events that broaden my knowledge and inform FinCEN of important perspectives. I have had the good fortune to meet with each of my counterpart leaders of the other federal financial regulators as well as a growing number of state regulators. I have also met with the leadership of many of our law enforcement agency partners, and I am making an effort to reach out to representatives of every constituent financial industry that is covered by FinCEN's regulations. I have also taken opportunities to address groups of examiners, compliance professionals, and both national and international industry leaders and executives in the US and in Europe. I am committed to continuing to focus a significant amount of FinCEN's resources to providing our partners with open channels and multiple vehicles for giving and receiving feedback. As you read this publication, please keep in mind the importance of feedback to our partnership for the protection of the financial system and feel free to pass along your thoughts.



James H. Freis, Jr.
Director
Financial Crimes Enforcement Network

Section 2 – Trends & 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 convenience checks, category “Other” on suspicious activity reports, and credit union cooperatives.

Contributors and Contributing Editors: Arlyne Warner, Michael de Luca, Jeremy Gahm, Jill Bezek, Nona Tiedge, and Rebecca Lassman

Trends in Suspicious Activity Reports Involving Convenience Checks

Credit card checks, also known as convenience checks or courtesy checks, are issued through a credit card company and linked to a credit card account. Customers find credit card checks convenient for use with merchants that do not accept credit cards, but do take checks. Credit card checks may be mailed to customers without the customer’s request. They do not require activation, thereby creating a heightened risk for identity theft by providing thieves an opportunity to gain access to customer’s information by simply stealing their mail. The thief only needs to sign the customer’s name on the face of the check and present it to any merchant. Customers may first learn of the identity theft when reviewing their credit card bills.¹

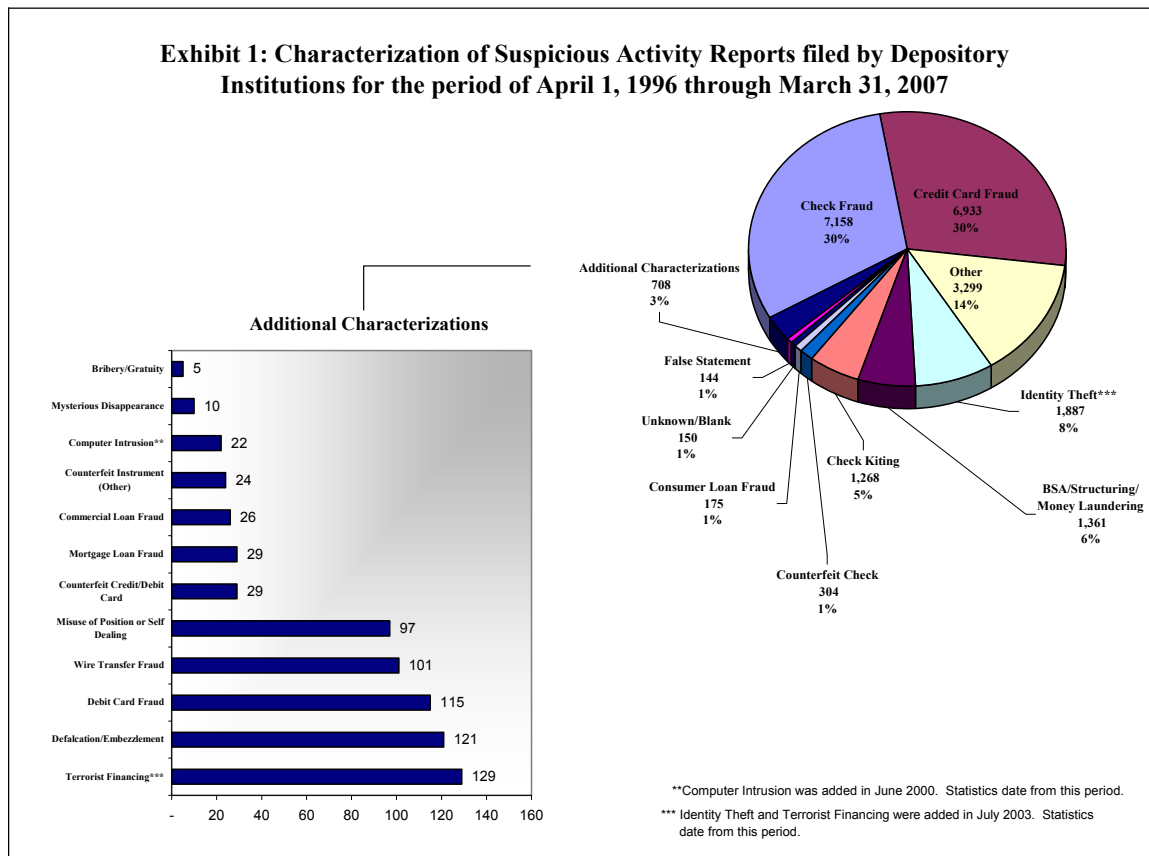
FinCEN conducted an assessment of Suspicious Activity Reports (SARs) filed during the period April 1, 1996 to March 31, 2007 with narratives containing three key search terms: “credit card checks”, “convenience checks,” and “courtesy checks.” The Bank Secrecy Act (BSA) database search produced 14,816 SARs. The reports can be broken down as follows:

- | | |
|--|--------|
| • Depository Institutions filed: | 14,670 |
| • Money Services Businesses filed: | 70 |
| • Casinos and Card Clubs filed: | 7 |
| • Securities and Futures Industries filed: | 69 |

¹ A convenience check may be tied to a credit card account, but it does not give a customer the same kind of consumer protection as a credit card. Regulation Z in the Truth in Lending Act (TILA), effective April 1, 2004, offers certain consumer protections for credit transactions. Currently, a convenience check is not treated as a credit card under Regulation Z because it can be used only once and not “from time to time” as a single transaction. For more information on Regulation Z go to: <http://www.federalreserve.gov/boarddocs/press/bcreg/2004/20040326/attachment.pdf>

Depository institution SARs showed the top 5 reasons for filing of suspicious activity² as:

Check Fraud	7,158 (30.61%)
Credit Card Fraud	6,933 (29.64%)
Other	3,299 (14.11%)
Identity Theft	1,887 (8.07%)
BSA/Structuring/Money Laundering	1,361 (5.82%)



Check fraud involved stolen convenience checks endorsed and deposited for illegal gain. Credit card fraud involved credit card “bust-out” schemes where the subjects opened credit accounts and quickly reached the credit limit. The subject then paid with a fraudulent convenience check to restore the credit balance and spent the limit again.

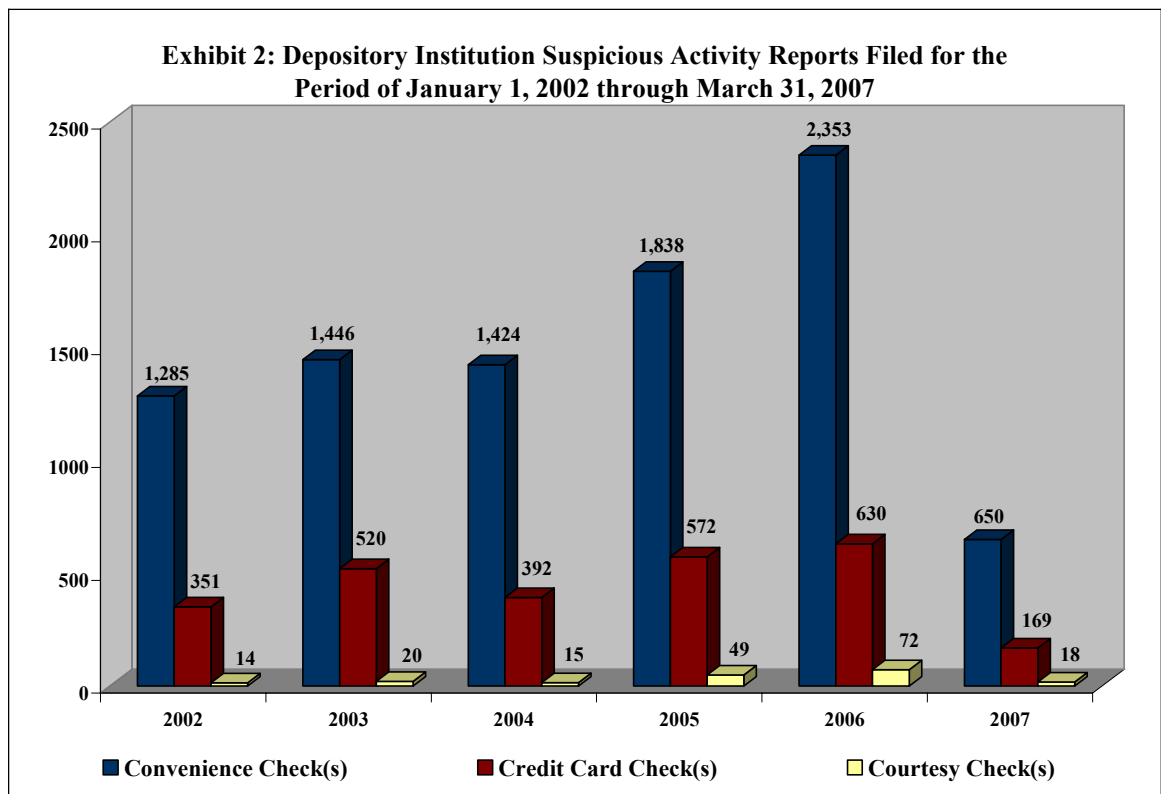
Two hundred and ninety-nine reports indicated check fraud and identity theft and described activity where the accounts were established using the victims’ names without their knowledge. In some cases subjects used their parents’ identities, and in other cases subjects used the identities of deceased persons to establish credit card accounts.

² Some SARs may list multiple suspicious activities.

BSA/Structuring/Money Laundering violations involved activities in which the subjects structured deposits and withdrawals of convenience, credit card, and courtesy checks. As soon as the funds were available, the suspect withdrew the funds, wrote checks, and made purchases. The financial institution sustained financial loss when the checks were later returned for insufficient funds.

Suspicious Activity Reports filed by Depository Institutions

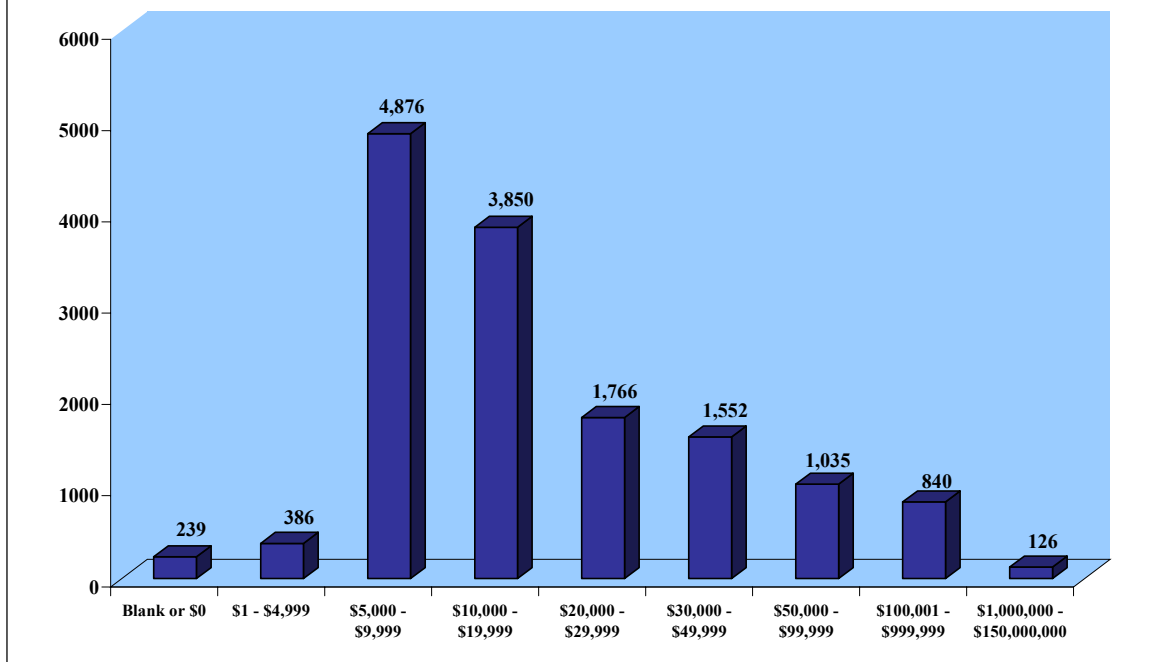
A search of the financial database for the period of April 1, 1996 through March 31, 2007 revealed 14,670 depository institution SARs filed with the specific search terms included in the narrative. Of those SARs, 11,245 listed convenience check(s); 3,163 listed credit card check(s); and 262 listed courtesy check(s). Exhibit 2 illustrates the activity by year.



Monetary Value Involved: The total dollar amount reported by depository institutions in the suspicious activity for the review period was \$1,153,551,294. One single filer reported an activity amount of \$150 million.³ Over 33% of the reports fell into the range between \$5,000 and \$9,999. Exhibit 3 illustrates the activity by dollar amounts.

³ The SAR narrative described two credit card checks, each written in the amount of \$75 million and dropped in a financial institution's after-hours depository.

Exhibit 3: Range of Activity Amounts from April 1, 1996 through March 31, 2007



Depository Institution SAR Narrative Analysis

A random sample of 1,745 (11.78%) narratives were analyzed to provide a statistical representation of the total SARs filed by depository institutions. The sample size was chosen to provide a confidence level of 95% with a confidence interval of +/- 3. A total of 2,218 distinct suspicious activities were reported on the sampled SARs.

A total of 796 (35.89%) of the sampled narratives reported “check fraud.” Specific activities described in those SARs include:

- Stolen convenience checks endorsed and deposited for illegal gain.
- Convenience checks counterfeited using computers, scanners, and copiers to create illegal checks.
- Checking accounts established using stolen identities and convenience checks at account opening. Checks subsequently issued from the account were returned for insufficient funds.
- Check kiting used in instances where the subject opened two or more accounts using convenience checks to create fraudulent balances.
- Convenience checks written on closed accounts.

A total of 762 (34.36%) of the sampled narratives reported “credit card fraud.” Specific activities described in those SARs include:

- Credit card bust-out schemes in which the subject opened a credit account and quickly reached the credit limit on the card, sometimes using credit card convenience checks for purchases. The subject then paid with a bad convenience check drawn on another account to restore the credit balance and spent the limit before the convenience check was returned again.
- Subject stole family member’s credit card checks.
- Stolen credit card checks deposited for illegal financial gain.

A total of 321 (14.47%) of the sampled narratives described other types of fraud:

- Check fraud and identity theft⁴ where credit card accounts were established in victim’s names without their knowledge. The fraud was discovered when the victim was contacted for restitution.
- Misuse of position in which the employee of the financial institution established accounts and deposited credit card convenience checks that were later returned for insufficient funds. When the checks were returned, the employee had deleted any record of the account.
- New accounts were used for credit card fraud and bust-out schemes. Subjects used the accounts to make large purchases, sometimes with convenience checks.

A total of 272 (12.26%) of the sampled narratives reported “identity theft.”

- Children used their parents’ identity to establish credit card accounts and subsequently received and used convenience checks issued by credit card companies,
- Subjects used the identity of deceased persons to establish credit card accounts and subsequently received and used convenience checks issued by credit card companies,
- Subjects illegally forged endorsements on credit card, convenience and courtesy checks that were stolen through the mail.

A total of 155 (6.99%) of the sampled narratives reported “BSA/Structuring/Money Laundering” as the suspicious activity:

- Subjects structured deposits and withdrawals of the convenience, credit card and courtesy checks. As soon as the funds were available, the suspect withdrew the funds, wrote checks, and made purchases. The financial institution sustained financial loss when the convenience checks were later returned for insufficient funds.

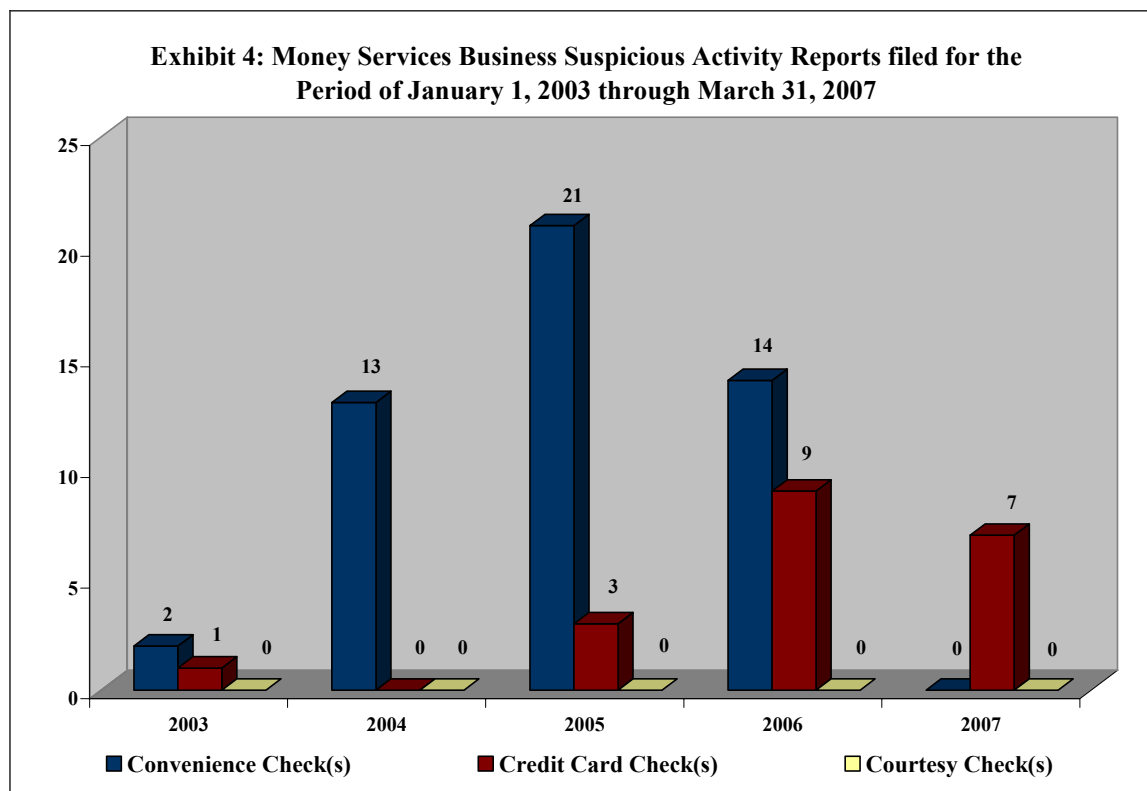
⁴ Identity theft was added in July 2003 and the characterization of suspicious activity “other” may have been used to report this type of activity until that time.

Other Institutions SAR Narrative Analysis

Of the 14,816 SARs produced for this analysis, only 146 were filed by money services businesses, casinos and card clubs, and securities and futures industries. Therefore, each individual narrative from these industries was evaluated for this analysis.

Money Services Businesses

The search resulted in 70 Suspicious Activity Report by Money Services Business (SAR-MSB) filings. Of those SAR-MSB filings, 50 listed convenience check(s), and 20 listed credit card check(s). No SAR-MSB narratives contained the term “courtesy check(s).” The total reported value in these SARs was \$865,019. Exhibit 4 illustrates the activity by year.⁵



The SAR-MSB narratives described the presentment of stolen convenience and credit card checks for cashing. The fraudulent activities include:

- Subjects presented stolen convenience and credit card checks in exchange for cash, alleging they had been paid for rendering services. The MSBs attempted to verify this by contacting the owners, who then advised that the checks were stolen. The MSBs contacted authorities. In two instances, the subjects were arrested.

⁵ For MSBs other than currency dealers or exchangers, the rule that requires the filing of SAR-MSBs applies to transactions occurring after December 31, 2001. However, no activity was reported in 2002.

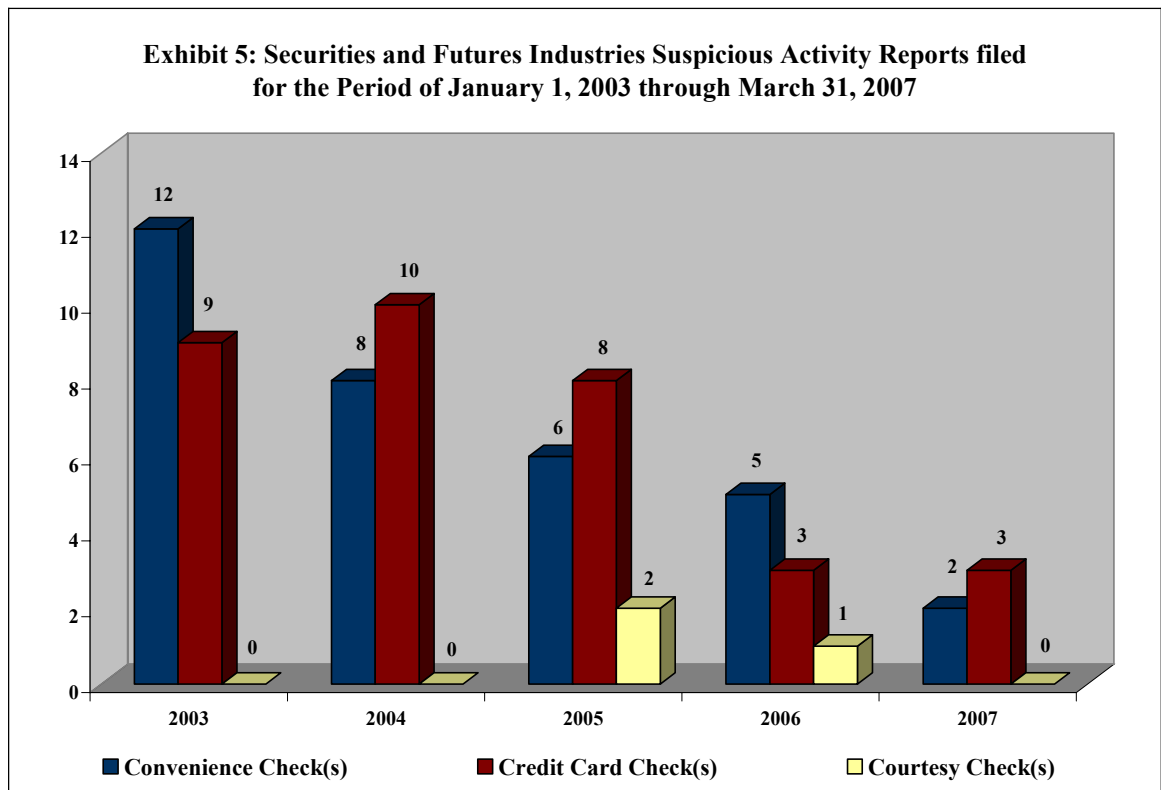
- The subject presented a stolen credit card check, alleging that it was payment for the sale of a vehicle. Upon request for a copy of the bill of sale, the subject terminated the transaction.

Casinos and Card Clubs

A search of the financial database revealed only seven Suspicious Activity Report by Casinos and Card Clubs (SAR-C) filings with narratives containing “convenience check(s),” “credit card check(s)” or “courtesy check(s).”

Securities and Futures Industries

There were 69 Suspicious Activity Report by Securities and Futures Industries (SAR-SF) filings identified. Of those SAR-SF filings, 33 listed convenience check(s), 33 listed credit card check(s), and 3 listed courtesy check(s). The total reported value in these SARs was \$14,632,261. Exhibit 5 illustrates the activity by year.



Activities reported include:

- Subjects presented third party credit card checks to deposit in their brokerage accounts. The funds were credited to their accounts. The subjects purchased stock, and then sold the stock for financial gain. The checks were later returned for insufficient funds or were reported as stolen. The brokerage company sustained financial loss.

- Subject(s) presented third party checks for deposit into their brokerage accounts. The checks cleared and funds were credited to their account. The deposited funds were debited by checks written on the account, wire transfers, and credit card purchases. The checks were later returned for insufficient funds or reported as stolen. The brokerage company sustained financial loss.
- Accounts opened using stolen credit cards, convenience, or courtesy checks that were later returned for insufficient funds or reported as stolen.

Use of the Category “Other” on Suspicious Activity Reports

Since the inception of the Suspicious Activity Reporting System in April 1996 through the end of 2006, filers have consistently selected *Other* from the listed types of suspicious activity on depository institution reports. In fact, *Other* currently ranks 3rd in the frequency of its selection amongst all available options. To select *Other* generally indicates that a suspected activity (in whole or in part) is not among the list of other summary characterizations currently made available in Part III of the SAR. Understandably, this list can not be infinite, hence the addition of *Other* as an available option.

Based on the variety of entries received over the years, the rationale of the *Other* fixed-field to act as a “catch-all” alternative in addition to and/or outside of the provided list of other summary characterizations has proven to be quite justified.

In 2006 there were 59,440 instances where *Other* was designated as the Characterization of Suspicious Activity (in whole or in part). In their description of *Other*, filers frequently noted the following activities: 1) Unregistered/ Unlicensed MSB; 2) Tax Evasion; 3) Fictitious Instrument(s); 4) Wire Transfer Fraud; 5) ITIN/SSN Fraud or Misuse; 6) Unusual [Cash] Activity; 7) Bank Fraud under 18 USC 1344; 8) Fraudulent W-2; 9) BSA/Structuring/Money Laundering; 10) Phishing and/or Spoofing; and 11) Automated Clearing House (ACH) Fraud.

The value of this information is extensive and useful to FinCEN as it provides insight on: Quality Control; Emerging Trends; Items of Strategic Interest; Due Diligence; Law Enforcement Support; and Reporting Patterns.

Quality Control

An examination of the details accompanying the selection of Other indicated that many SARs were filed improperly.

Improper entries included: comment to *See Attached* (or similar); one-word descriptions that were too broad (e.g., *Fraud*; *Scam*); or fragmentary information in support of the selected characterization (e.g. *Unusual Activity*; *Suspicious*;

Fraud Ring; Money Orders). In several instances the description portion of the *Other* field was left blank. Although additional information can be, and in many cases was, provided in the narrative portion of the report, a blank, incomplete, confusing, or otherwise inadequate entry in the description section of the *Other* fixed-field make the SAR less searchable by law enforcement and the regulatory community. Entries made in the Summary Characterization and the SAR Narrative are not mutually exclusive. On the contrary, data populating the fixed-field sections of the SAR must support the explanation provided and vice versa.

In addition, there were descriptions that indicated the filing of Suspicious Activity Reports was unnecessary. For example, there were SARs that contained the following descriptions: *Robbery; Insufficient Funds/Overdraft; Mail Fraud; Bank Error*. A SAR is not required for a robbery or burglary committed or attempted as long as it is reported to appropriate law enforcement (see 31 CFR 103.17(c)(1)(i); 103.18(c); 103.19(c)(1)(i); and 103.21(c)). Descriptions in other reports, though less common, included supporting explanations such as: *Non Fraud* or *No Fraud Found*.

A number of explanations for use of the *Other* category contained the phrase *Subpoena* or *Grand Jury Subpoena*. FinCEN has issued guidance on Grand Jury Subpoenas, indicating the mere receipt of any law enforcement inquiry does not, by itself, require the filing of a Suspicious Activity Report. Nonetheless, a law enforcement inquiry may cause a financial institution to review the activity for the relevant customer. It is incumbent upon a financial institution to assess all of the information it knows about its customer, including the receipt of a law enforcement inquiry, when determining whether a SAR should be filed. Further information regarding FinCEN's guidance on Grand Jury Subpoenas and Suspicious Activity Reporting may be found at: <http://www.fincen.gov/sarreviewissue10.pdf>.

Emerging Trends & Items of Strategic Interest

The breadth of descriptions contained within the “catch-all” characterization of *Other* act as a barometer for a variety of known financial schemes, alerting us to the emergence of new trends, as well as identifying original ones. This information enables us to strategically conduct additional, in-depth research on critical themes.

In 2005, for example, descriptions of activities characterized as *Other* indicated certain emerging trends, including: *Automated Clearing House (ACH) Fraud; Phishing or Spoofing Scams; and Financial Abuse of the Elderly* (commonly listed as *Elder Abuse*). Through identifying trends in the *Other* field, FinCEN can prioritize emerging issues due to their reported frequency and the serious nature of the activity, e.g., *Fictitious Instrument(s) and Lottery-Sweepstakes Scams*.

Due Diligence

The frequency with which known and suspected *Unregistered or Unlicensed Money Services Businesses* were identified is evidence of due diligence and awareness on the part of the filing industry in recognizing and reporting such entities.

Law Enforcement Support

Several *Other* types of suspicious activity are regularly indicated and are of enormous value to specific law enforcement agencies, such as: *Tax Evasion; Fraudulent W-2; Narcotics Trafficking; Currency Smuggling; and Employing Illegal Aliens.*

Reporting Patterns

Filers utilizing the *Other* fixed-field could have been more accurate and descriptive by clearly designating a more appropriate category: *Wire Transfer Fraud; BSA/ Structuring/ Money Laundering; Counterfeit Instrument (Other); Mortgage Loan Fraud; or Identity Theft.*

Moreover, several explanations involved *Advanced Fee Scams* or the *Office of Foreign Assets Control (OFAC)*. FinCEN has published guidance related to Advanced Fee Scams (commonly referred to as Nigerian or 419 Scams). To consult these guidelines please refer to Issues 4 and 7 of the *SAR Activity Review*. Access to this publication may also be obtained via the following link:

<http://www.fincen.gov/sarreviewissue4.pdf> and
<http://www.fincen.gov/sarreviewissue7.pdf>.

In December 2004, FinCEN released interpretive guidance concerning reports filed related to the Department of the Treasury's Office of Foreign Assets Control ("OFAC"). Details of this guidance may be reviewed in full via:

<http://www.fincen.gov/sarguidanceofac.html>.

Conclusion

There can be no doubt as to the all-around usefulness of the wide reporting discretion offered by the *Other* characterization box and its descriptive line. The presented observations not only emphasize this, but also point out how the *Other* field can be more accurately used, specifically in those instances where the type of suspected violation is already offered as one of the other listed summary characterizations. Choosing the relevant available violation will additionally make for more accurate numeric tabulations and a better representation of those summary characterizations.

Credit Union Cooperatives

This section of *The SAR Activity Review* outlines findings from Suspicious Activity Reports referencing credit union cooperatives that provide shared-branching services to member credit unions.

Credit Union Cooperative Shared-Branching Model

Credit union cooperatives operate networks that provide Electronic Funds Transfer/Automated Teller Machine/Point of Sale (EFT/ATM/POS) and shared-branching services to the cooperatives' member credit unions. Where applicable, cooperatives' EFT/ATM/POS networks enable members of participating credit unions to use other participating credit unions' ATMs without paying fees or on a reduced-fee basis. Shared branches allow members of participating credit unions to conduct transactions at either branches of the cooperative's other participating credit unions or facilities that are managed by the cooperative itself.

There are three types of shared branches:⁶

- **Outlet** – A facility owned and staffed by a credit union where members of other credit unions, within the same cooperative network, can conduct transactions.
- **Stand-Alone** – A facility owned and staffed by a credit union cooperative, where members of participating credit unions can conduct transactions.
- **Partnership Outlet** – A facility owned by a credit union or group of credit unions and staffed by employees of the cooperative, where members of participating credit unions can conduct transactions.

Credit unions belonging to shared-branching networks fall into two categories:

- **Issuer** – Credit unions that allow their members to conduct account transactions, transfers, or payments at other outlets, partnership outlets, and stand-alones within the same shared-branching network.
- **Acquirer (Issuer/Acquirer)** – Issuers that serve as outlets by accepting and processing transactions from members of other credit unions within the same shared-branching network.

In a given transaction, the issuing credit union pays a fee to the acquiring credit union. If the transaction occurs at a shared-branching facility that is operated by the cooperative, the issuing credit union pays a fee to the cooperative. The cooperative annually distributes its income collected from fees to its stockholders. Credit union cooperative shareholders can be credit unions, corporate/industrial credit unions, state credit union leagues, or other credit union service organizations.

⁶ Swedberg, Jamie. "Share and Share Alike." *Credit Union Management*. January 2006. pg. 38; and Dernovsek, Darla. "Shared Branching Takes Root." *Credit Union Magazine*. November 2005. pp. 44-47.

Synopsis of SAR Filing Activity: Credit Union Cooperatives

FinCEN researched SAR filings referencing credit union cooperatives for the period June 2004 through March 2007. The research addressed SARs filed by other financial institutions with narrative references to credit union cooperatives and terms related to terrorist financing, organized crime, fraud, scams, or money laundering. In addition, information about the cooperatives' structures and Bank Secrecy Act (BSA) compliance policies were reviewed.

FinCEN's database queries produced 121 SARs with narrative references to credit union cooperatives and terms related to terrorist financing, organized crime, fraud, scams, or money laundering:

- Twenty-three depository institution SARs filed by credit union cooperatives;
- Four depository institution SARs and four SARs by Money Services Business (SAR-MSBs) that identified some name derivative of a credit union cooperative as a subject;
- Seventy-eight depository institution SARs and ten SAR-MSBs with narrative references to one of the cooperatives and terms related to fraud, scams, or money laundering; and
- Other instances where credit unions apparently incorrectly filed a SAR-MSB and a SAR by Securities and Futures Industries (SAR-SF) that described shared-branching transactions.

The cooperatives' SAR filings demonstrated several errors including a potential lack of consistency in the use of filer names and Federal Employer Identification Numbers (FEINs). The twenty-three depository institution SAR filings contained sixteen different filer name variations, ten different filer FEINs, and seventeen different combinations of FEINs and filer names. Analysis identified other errors in 15 of the 23 depository institution SAR filings.

Fifty of the 121 (41.32%) SAR filings with some connection to the credit union cooperatives involved fraud or attempted fraud. Seven of the 23 filings (30.43%) by cooperatives involved alleged frauds.

Details on SARs Filed by Credit Union Cooperatives

Several facts about the 78 depository institution SARs and 10 SAR-MSBs with cooperative narrative references appear noteworthy. One SAR-MSB identified an elaborate plot to launder stolen funds using shared branches to deposit cash into a digital currency account holder's credit union account. Sixty-two of the 78 (79.49%) depository institution SARs and five of the ten (50%) SAR-MSBs identified credit union account holders as subjects. Thirty-nine of the 78 (50%) depository institution SARs alleged that a credit union account holder was attempting to launder funds. Eight of the ten SAR-MSBs involved money laundering as well.

Twenty-seven of the 78 (34.62%) depository institution SAR filings with narrative references to the credit union cooperatives involved transactions occurring at multiple shared-branching locations. Twenty-two of these 78 (28.21%) named members of participating credit unions as subjects. Fourteen SARs involving multiple shared branches contained narrative references to money laundering or structuring. Thirteen filings involving multiple shared branches had narrative references to frauds or attempted frauds.

Queries produced 23 depository institution SARs filed from June 2, 2004 through March 6, 2007 by the credit union cooperatives covered in this study. The reports had a total of 16 unique filer-name variations, 10 unique FEINs, and 17 unique combinations of the two.

At least 65.21 percent of SARs filed by credit union cooperatives contained other potential data quality problems. Approximately 30.43 percent of the total filings had either blank or incomplete narrative fields. Some filers attempted to place narratives in the *Violation Type Other* field. Some reports contained the wrong *Branch Address*, wrong *Total dollar amount involved in known or suspicious activity*, or lacked FEINs. Other filers inserted “please see attached” in the SAR narrative and listed *Armed Robbery* as the characterization of suspicious activity. As a reminder, when SAR forms are received at the Enterprise Computing Center-Detroit, only information that is in an explicit, narrative format is entered into the system; thus, tables, spreadsheets or other attachments are not entered into the SAR System database.

Table 1 displays the different characterizations of suspicious activity found in the 23 depository institution SAR filings (some reports contained multiple characterizations).

Table 1: Cooperative SAR Filings – Characterization of Suspicious Activity

Characterization of Suspicious Activity	# of Reports with Characterization	% of Reports with Characterization
Other	8	34.78%
BSA/Structuring/Money Laundering	8	34.78%
Check Fraud	4	17.39%
Misuse Of Position Or Self-Dealing	4	17.39%
Defalcation/Embezzlement	3	13.04%
Check Kiting	3	13.04%
Mysterious Disappearance	1	4.35%
Counterfeit Check	1	4.35%

Explanations of the covered cooperative depository institution SAR filings with “Other” as the characterization of suspicious activity included the following:

- “Armed Robbery”
- “Money Order Fraud”
- “Rejected Wire OFAC List”
- “OFAC Hit”
- “Avoid Filling Out CTR”
- “4 Separate Cash Deposits”
- “Deposited 9000 00 Cash In Acct He Holds”
- “Made Two Cash Deposits To An Account He”

Depository Institution SARs with Credit Union Cooperatives Narrative References

Research identified 78 depository institution SAR narratives involving covered cooperatives and terms related to fraud, scams, or money laundering that did not solely involve unconfirmed structuring.⁷ Sixty-two of the 78 (79.49%) filings named members of participating credit unions as subjects. Research did not locate any SARs where the filer described a financial activity as being related to terrorist financing, terrorist groups, or organized crime. *Table 2* contains a summary of filer characterizations of suspicious activity.

Table 2: Depository Institution SAR Narratives Referring to Credit Union Cooperatives – Characterizations of Suspicious Activity

Characterization of Suspicious Activity	Count	% of Total	With Credit Union–Member Subject	% of Total
BSA/Structuring/Money Laundering	45	48.39%	39	41.94%
Counterfeit Check	16	17.20%	12	12.90%
Check Fraud	12	12.90%	10	10.75%
Other	6	6.45%	4	4.30%
Check Kiting	5	5.38%	5	5.38%
Counterfeit Instrument (Other)	4	4.30%	1	1.08%
Wire Transfer Fraud	2	2.15%	2	2.15%
Debit Card Fraud	2	2.15%	2	2.15%
Credit Card Fraud	1	1.08%		
TOTAL	93	100.00%	75	80.65%

⁷ Some SARs involving structuring, that described subjects inquiring about CTR limits or cut-off times for aggregating transactions, were included in this count.

Thirty-four depository institution SAR narratives, or 43.59 percent of the total filings, involved frauds or attempted frauds. Twenty-six of the SARs filed involving fraud or attempted fraud, or 33.33 percent of the total filings, identified members of participating credit unions as subjects. Seven filings described alleged 419 scams. Four of these seven filings named members of participating credit unions as subjects. The remaining three involved counterfeit instruments drawn on one of the cooperatives. In one instance the individual allegedly was perpetrating a 419 scam⁸ and advised the potential victim to attempt to cash a \$6,500 counterfeit check at a specific shared branch. *Table 3* contains a summary of filings involving different types of fraud. The characterizations in this table were drawn from descriptions of suspicious activities in SAR narratives.

Table 3: Depository Institution SAR Narratives Referring to Credit Union Cooperatives – Characterizations of Suspicious Activity Involving Frauds

Characterization of Suspicious Activity	Count	% of Total	With Credit Union–Member Subject	% of Total
Check Fraud	10	12.82%	9	11.54%
Counterfeit Check	9	11.54%	6	7.69%
Nigerian Scam and Check Fraud	4	5.13%	1	1.54%
Check Kiting	4	5.13%	4	5.13%
Counterfeit Checks and Debit Card Fraud	2	2.56%	2	2.56%
Nigerian Scam, Check Fraud, and Counterfeit Money Orders	1	1.28%	1	1.28%
Nigerian Scam and Money Laundering	1	1.28%	1	1.28%
Nigerian Scam	1	1.28%	1	1.28%
Check Fraud and Money Laundering	1	1.28%	1	1.28%
ATM Fraud, Check Kiting, and Check Fraud	1	1.28%	1	1.28%
Total:	34	43.59%	26	33.33%

⁸ In the “Advance Fee Fraud” or 419 schemes, victims may receive emails and letters from groups of con artists located in Nigeria who claim to have access to a very large sum of money and want to use the victim’s bank account to transfer the funds. In exchange for the victim’s services, they claim they will give the recipient of the email/letter a large percentage of the funds. These schemes have a common denominator - eventually the target of the scheme will be required to pay up-front (advance) fees (licensing fees, taxes, attorney fees, transaction fees, bribes, etc.) to receive the percentage of funds promised. The con artists usually request that they be furnished with blank company letterhead and/or bank account information.

Sixty-one different financial institutions filed the 78 depository institution SARs discussed in this section. The 78 depository institution SAR narratives contained a total of eight different references to credit union cooperatives and affiliated entities covered in this study.

Table 4 provides a statistical breakdown of the number of different shared-branching locations involved in the 78 depository institution SAR filings. Twenty-seven reports, or 34.61 percent of the total filings, involved transactions that occurred at multiple shared-branching locations. Twenty-two of these reports, or 28.21 percent of the total filings, named members of cooperative-participant credit unions as subjects. Fourteen filings involving multiple shared-branching locations contained narrative references to money laundering or structuring. Thirteen filings involving multiple shared branching locations had narrative references to frauds or attempted frauds.

Table 4: DI SAR Narrative Referring to Covered Credit Union Cooperatives – Breakdown of Shared-Branching-Transaction Locations

Shared-Branching-Transaction Locations	DI SAR Filings	% of Total	With Credit Union-Member Subject	% of Total
0	4	5.13%	0	0.00%
1	47	60.26%	40	51.28%
2	9	11.54%	6	7.69%
3	14	17.95%	12	15.38%
5	2	2.56%	2	2.56%
6	2	2.56%	2	2.56%
Total:	78	100.00%	62	79.49%

Conclusion

FinCEN’s research on SAR filings for credit union cooperatives provides an indication of the selected characterizations of suspicious activities currently being identified within the credit union industry. FinCEN’s research also indicates that credit union cooperatives’ SAR filings demonstrate a potential lack of consistency in the use of filer names and FEINs, in addition to other errors. The number of filer-name and FEIN variations in BSA filings related to these cooperatives could complicate future efforts to correctly identify and aggregate SAR filings involving the cooperatives and their affiliated entities. Data consistency problems and other data-quality issues prolonged and hindered efforts to collect and evaluate data for this analysis.

In many cases, filers already have the information to correct errors, hence they can improve the value of SARs to the law enforcement community at little or no cost to the institution. FinCEN recently issued guidance on “Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting.”

http://www.fincen.gov/SAR_Common_Errors_Web_Posting.pdf

Section 3 – Law Enforcement Cases

This section of *The SAR Activity Review* affords law enforcement agencies the opportunity to summarize investigations where Suspicious Activity Reports (SARs) and other BSA information played an important role in the successful investigation and prosecution of criminal activity. This issue contains 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.

Contributing Editors: Jack Cunniff, James Emery, Shawn Braszo

Law Enforcement Contributors: The requirements of confidentiality relating to SARs preclude FinCEN from associating the name of all of the law enforcement agencies that made creative, appropriate use of SAR information with the cases highlighted in this issue. However, in addition to the investigating agencies noted at the end of each case, the following agencies contributed to the cases in this issue: Internal Revenue Service, U.S. Immigration and Customs Enforcement, Bureau of Alcohol, Tobacco, and Firearms, Drug Enforcement Administration, Federal Bureau of Investigation, Social Security Administration, Environmental Protection Agency, United States Postal Inspection Service, United States Secret Service, the Eastern District of California SAR Review Team, and the Northern Virginia SAR Review Team.

SUSPICIOUS ACTIVITY REPORT LEADS TO THE INVESTIGATION AND CONVICTION OF ELECTED OFFICIAL

A bank filed a SAR on an elected official from a suburban locality who structured transactions totaling hundreds of thousands of dollars. The SAR triggered an investigation that confirmed the structuring and identified evidence that the elected official committed perjury while filing a bankruptcy petition. Additional SARs filed on the defendant detail structuring at the bank as well as at a money services business.

A federal jury found the official guilty of 32 counts of bankruptcy fraud and illegal structuring of cash. State law required the defendant to resign because of the conviction.

The defendant had previously filed for bankruptcy, which prosecutors said was an effort to eliminate credit card debts. Prosecutors charged him with lying to his bankruptcy lawyer and concealing the ownership of his home that he and family members purchased. In addition, prosecutors said that the defendant concealed his private business and bank accounts from the bankruptcy court. During those proceedings, he claimed only his official salary as income.

Even though the defendant claimed he was bankrupt, in an 18-month period he made over 1,000 deposits at several different bank locations into his accounts totaling more than \$500,000. His defense attorney stated that his business dealings took place throughout a large area, making cash transactions at different locations a necessity and not a means of attempting to avoid reporting requirements.

However, his bank thought differently. After reviewing the transactions that occurred over an extended period of time, the institution filed a SAR and simultaneously notified the Internal Revenue Service (IRS). Within the next month, the bank filed two additional SARs, and a check casher filed another.

The SARs detail transactions taking place at several different locations in amounts less than \$10,000 and, in one instance, five transactions occurring in one business day. The defendant was making cash deposits totaling up to \$30,000 monthly and writing numerous \$2,000 checks to himself and family members.

Because of the defendant's use of both a bank and a check casher, investigators believe that he may have been undertaking an elaborate check-kiting scheme. In fact, his complex practices resulted in more than \$90,000 in check cashing fees.

A lengthy indictment details 24 separate counts of structuring. The indictment details both currency deposited at the bank and checks cashed at a currency exchange business. The transactions range from \$11,000 to nearly \$30,000.

(Investigating Agency: Internal Revenue Service)

SUSPICIOUS ACTIVITY REPORT DETAILS ILLICIT CHECK CASHING ACTIVITY, PROVIDES BLUEPRINT FOR INVESTIGATION AND INDICTMENT

In the course of an investigation into possible terrorist activities, investigators uncovered a SAR that provided detailed information concerning suspect check cashing activity by the operators of a convenience store. The filing bank's audit found that the business was cashing checks to disguise payments to illegal workers in the construction industry. In addition, the bank's audit and the subsequent law enforcement investigation found the business failed to complete Currency Transaction Reports (CTRs).

The local United States Attorney announced the indictment and arrests of two individuals in 2006. The 115-count indictment charges that in association with their business, the individuals committed numerous money laundering offenses. Court documents show the defendants failed to file CTRs, failed to register with FinCEN, and structured transactions to avoid detection. Moreover, much of the illicit financial activity was designed to conceal, harbor, and shield illegal aliens.

The case began in the aftermath of the September 11 terrorist attacks. The Bureau of Alcohol, Tobacco & Firearms received a tip that associates of the defendants were involved in illegal gun sales to the Middle East. A joint

investigation of federal, state, and local agencies soon identified the defendants and possible suspicious money transfers from their business. When the investigation linked the defendants to improper payments made to illegal aliens (after retrieving the SAR from the Bank Secrecy Act database), U.S. Immigration and Customs Enforcement took the lead.

That SAR proved to be the big break in the case. The bank filed the SAR for transactions that occurred during one month in 2002, the timeframe for its audit. In the SAR, the bank noted that the store provided check cashing services to select customers, namely in the construction industry. Normal activity included daily deposits of large volumes of third party checks and corresponding withdrawals of the currency either at bank branches or via armored car deliveries. The bank performed an audit on the business, as a routine matter, for transactions that occurred that month. The bank found that the business did not consistently complete CTRs, or when they did, the records were not sent to FinCEN. Furthermore, transactions involving three companies did not generate any CTRs. Those transactions totaled approximately \$900,000 for that month alone.

Investigators used that SAR as the basis for a grand jury subpoena and eventually as the blueprint for the indictment. Many parts of the bank's detailed audit are included in the indictment. Notably, the first 100 counts of the indictment are 100 transactions that occurred during the month of the audit. In all, investigators concluded that the defendants were cashing millions of dollars of checks per month at the convenience store. Investigators point to this case as an example of how to get an indictment from a SAR, or in their terms, "indict the SAR."

The illegal check cashing supported two criminal activities. First, construction companies cashed checks there to facilitate the payment to unauthorized workers and illegal aliens. Second, many construction companies used the check cashing business to pay workers in cash and avoid the payment of payroll taxes, in particular workers' compensation insurance. In some areas, the cost of that insurance can be as high as 50% for trades such as roofing. Investigators found evidence that construction companies from different parts of the state traveled to the convenience store to cash checks.

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

SUSPICIOUS ACTIVITY REPORTS DOCUMENT TRANSACTIONS BY DEFENDANT WITH TIES TO ORGANIZED CRIME GROUP, POSSIBLE TERRORISM FINANCING

An illegal alien pleaded guilty to stealing Social Security numbers, fabricating names, and swindling almost \$2 million dollars from credit card companies. The defendant's name surfaced in the course of an investigation into organized criminal activity. Suspicious Activity Reports document some of the most serious charges against the defendant.

In late 2006, a federal judge sentenced the defendant to four years in prison for his role in a credit card fraud ring that bilked more than \$1.7 million from credit card companies using stolen Social Security numbers and fictitious names. The judge indicated that the defendant, a Lebanese national, is an illegal alien who came into the United States from Mexico and has ordered him deported following the completion of his sentence.

The defendant pleaded guilty earlier to conspiracy to commit credit card fraud and aggravated identity theft. The charges arose out of a search of his apartment by the Federal Bureau of Investigation during which agents discovered dozens of credit cards and identity profiles. They also seized mail from six different commercial mailboxes where the defendant received mail from credit card companies in fictitious names.

Further investigation determined that the defendant obtained credit cards with the help of stolen Social Security numbers and fictitious names. In doing so, he was able to transfer balances, receive cash, and make purchases such as the \$12,000 he supposedly used for hair implants.

Three financial institutions filed SARs on the defendant citing check kiting and credit card fraud as the suspect activity. In addition to listing instances of the defendant passing bad checks, one SAR noted that the defendant had opened 13 accounts within a 24-month period and revolved funds totaling more than \$70,000 on these accounts. Another SAR noted large funds transfers to Lebanon.

(Investigating Agency: Federal Bureau of Investigation)

BSA RECORDS, 314(A) REQUEST ASSIST INVESTIGATION OF INTERNATIONAL MONEY LAUNDERING USING STORED VALUE CARDS

A man accused of managing an international theft ring involving more than \$1 million has been indicted and faces charges including fraud and money laundering. Prosecutors allege that the defendant stole the identities of hundreds of people and used his stored-value card business to launder and transfer funds to Russia and elsewhere. Bank Secrecy Act records helped investigators piece together the investigation and provided additional leads.

In late 2006, a federal grand jury indicted the defendant on 152 counts of wire fraud, money laundering, and identity theft. The government charges that he established a company in the business of selling stored-valued ATM cards and that he allegedly swindled unsuspecting victims using their bank account and credit card information.

Customers set up electronic payment accounts in order to simplify their transactions. Investigators said that the defendant's co-conspirators assisted in the scheme by obtaining bank account and credit card information from victims and then stealing from their accounts. The stolen funds were then given to the defendant who in turn deposited the money into his stored-value cards. These cards were gift cards

that acted as debit cards and carried the names of the victims whose identities had been stolen. In order to further carry out his scheme, the defendant transferred the money from one account to another which made tracing the funds difficult for investigators. Fifteen cards were held in the United States and six cards were sent to Russia. The co-conspirators would then retrieve the money from ATM machines.

Prosecutors note that in 1998 the defendant filed for bankruptcy stating that in the previous year his income was only \$10,000, but he had more than \$55,000 of debt. However, within a few years, he was able to purchase a home valued at more than \$1 million in a gated community. He also owned a new Lexus automobile and frequently vacationed in Las Vegas. The Federal Bureau of Investigation (FBI) seized the house and the car along with \$160,000 in cash.

The defendant originally started the business in question on-line. He later incorporated the business and attempted to sell stock in the corporation. That effort resulted in a cease and desist order. He later converted his business into a provider of stored-value cards. Through Internet bulletin boards, he attempted to solicit distributors for his service. The defendant attracted the attention of financial institutions, who originally contacted the Drug Enforcement Administration (DEA) because of the suspicious nature of the transactions.

The investigation started when the filer noticed suspicious activity that occurred in December 2002 associated with the defendant, filed a SAR, and notified the DEA. The activity, which included computer intrusion, credit card fraud, debit card fraud, and wire transfer fraud, involved numerous accounts for relatively low amounts of money. Apparently, the filer believed the activity was consistent with transactions associated with illegal drug activity and thus contacted the DEA.

The FBI, IRS, ICE, and state and local agencies eventually joined the task force investigation. Agents believe the defendant used his company to launder and transfer monies estimated to be close to \$1 million through Europe, the U.S., and former Soviet republics. The defendant perpetrated the scheme through the identity theft of hundreds of Americans and numerous bank frauds.

An FBI agent assigned to the case said that BSA records provided information that led to the subpoena of records from individuals, businesses, and banks. Those records in turn eventually led to the defendant's indictment.

(Investigating Agencies: Drug Enforcement Administration, Federal Bureau of Investigation, Internal Revenue Service, U.S. Immigration and Customs Enforcement)

SUSPICIOUS ACTIVITY REPORT LEADS TO GUILTY PLEA IN STRUCTURING CASE

In a case that started from a proactive review of SARs, an automobile dealership pleaded guilty to conducting transactions designed to avoid the filing of Currency Transaction Reports. Although the SAR only details activity that occurred in

a period of twenty days, investigators found a pattern of transactions where the business engaged in a process to sell autos while ignoring and violating Bank Secrecy Act (BSA) requirements as well as avoiding traditional financing arrangements. Less than one year passed from the time the financial institution filed a SAR to when the corporate entity entered a guilty plea.

In late 2006, an automobile dealership pleaded guilty to structuring cash deposits. The business faced a maximum term of five years probation, a fine of \$50,000, and a special assessment.

According to court documents, between April 2005 and January 2006, the business structured 20 cash deposits totaling over \$400,000 into the company's bank account. As part of the plea agreement, the corporation also forfeited over \$325,000 to the U.S. Government. This amount is in addition to almost \$70,000 administratively forfeited.

The reporting financial institution noted that on twelve occasions in December 2005, the business conducted transactions where an amount of currency just under the reporting requirement was deposited into the business's account. The amount of currency ranged from \$7,000 to over \$9,000 and the total deposits for each day ranged from almost \$11,000 to just under \$20,000.

Investigators found that the business dealt strictly with used cars. Normally, the defendants arranged for the sale of cars through cash payments and in-house financing. Buyers would typically pay a large portion in cash, up to \$9,000, and finance the rest in \$350 payments. The business performed no background or credit checks on buyers, nor did they complete any Bank Secrecy Act forms on the auto sales.

The reporting bank completed a SAR in late 2005, and investigators reviewed it in February 2006. Investigators conducted a seizure in April of that year and conducted interviews in May. Based on the evidence the investigators had, the corporation agreed to a pre-indictment plea in late 2006.

(Investigating Agency: Internal Revenue Service)

SUSPICIOUS ACTIVITY REPORTS DETAIL TRANSACTIONS IN MORTGAGE FRAUD SCHEME

A federal judge has ordered more than 24 years of prison time for a former loan officer who was found guilty on all eight counts of an indictment charging conspiracy, bank fraud, wire fraud, and money laundering. Several financial institutions identified unusual transactions related to the defendant and filed SARs. These SARs proved very helpful during the investigation.

In addition to prison time, the judge ordered three years of supervised release and for the defendant to pay restitution of over \$5,000,000 as well as a monetary judgment of more than \$1.5 million.

The government's evidence at trial established that from 2002 to 2003 the defendant organized a conspiracy to "flip" over 30 residential properties, a scheme which netted over \$5 million for the defendant. The defendant worked as a loan officer for a lender and through this position submitted loan applications for straw buyers seeking approximately \$14 million in loans to purchase the properties. These loan applications falsely listed the straw buyers' assets, income, and other information.

The defendant paid a co-defendant to write dishonest appraisals falsely reporting the conditions of the properties and stating that the properties were renovated when, in fact, they were not. The co-defendant, who was not even a licensed appraiser, stole actual appraisers' names and licenses to write completely fabricated reports on the value of the houses. These fraudulently inflated appraisals caused the banks to loan inappropriately high mortgages. The co-defendant pleaded guilty to conspiracy to commit bank fraud and received a prison sentence of 46 months.

In the beginning of the scheme, co-conspirators worked as underwriters at the lender employing the defendant. The co-conspirators approved loans that did not meet the banks' requirements and were paid by the defendant to do so.

By using the false loan applications, the inflated appraisals, and the fraudulently obtained underwriting, the defendant and the co-conspirators caused the banks to issue loans to the straw buyers in amounts that were much higher than the value of the underlying properties, thus creating a large amount of illegal proceeds when the properties were "flipped" to the buyers. Another co-conspirator purchased the properties, and, many times on the same day, quickly resold the "flipped" properties to the straw buyers at the price of the inflated appraisals. In this manner, a huge amount of money was generated for the co-conspirators. In one day, a single property could produce between \$150,000 and \$400,000 of cash for the conspiracy.

The defendant received the majority of the ill-gotten gains. At times this money was identified on the settlement statements as reimbursement for "rehab construction," when, in truth, no renovations had been performed and little if any rehab was ever carried out on the properties. Instead, the defendant used the money to live a lavish lifestyle, to pay off the co-conspirators, and to fund the continuation of the conspiracy. The mortgages on all but one of the 32 properties defaulted and foreclosed or sold before foreclosure for a loss. The banks resold the properties (in a strong real estate market) but for less than the amount of the mortgage loans. After resale, the banks were left with a loss in excess of \$5 million.

In 2003, the parent company of the lender filed a SAR on the defendant noting a series of suspect mortgage loans. The SAR noted that 17 of 25 loans had common borrowers. In addition, the loans often included the same sellers, underwriters, and appraisers. Furthermore, the bank discovered that many of the so-called renovations were never done and that money allegedly paid for renovations was in

fact sent to a corporation controlled by the defendant. A SAR filed in 2006 reports the loss on some of the loans that the defendant originated. Also in 2006, a bank filed a SAR alleging that the defendant stole the identity of a woman and used that information to buy several vehicles.

(Investigating Agency: Federal Bureau of Investigation)

SUSPICIOUS ACTIVITY REPORTS “EXTREMELY HELPFUL” IN STRUCTURING CONVICTION RELATED TO INTERNATIONAL LOTTERY SCHEME

In what a federal prosecutor called “the most blatant currency structuring case” he had seen, a federal judge sentenced an 82-year-old man in March 2007 to 15 months in prison and ordered him to pay \$110,000 in restitution to American victims of an international lottery scheme. The defendant had been involved in several suspicious investment schemes over the past few years, and numerous SARs document a string of unusual transactions. In addition, the investigating FBI agent reported that he would not have been able to make the case without the SARs.

The defendant told a U.S. district judge that he regretted his involvement in the case, which is still being investigated by Canadian law enforcement. Prosecutors charged that the defendant and his Canadian partners, none of whom have been apprehended, ran “an online scam” on the Internet involving false enticements pertinent to the Australian Lottery.

As part of his plea agreement, the defendant admitted that he structured cash withdrawals from his bank, in amounts less than \$10,000, for the purpose of evading reporting requirements of the BSA. He specifically admitted that he was aware of the CTR threshold.

The defendant claimed to be the intermediary in the scheme. Victims would send money to him, mostly through wire transfers and personal checks that he deposited in various accounts, and he would withdraw the money in structured transactions. With cash in hand, he would purchase money orders to send to the principals in the scheme. In consideration of the defendant’s age, the assistant U.S. attorney suggested a term between 12 and 18 months in the U.S. Bureau of Prisons, although the usual guideline for that crime would be 33 to 41 months. “This is the most blatant currency structuring case I have ever seen in my career,” the prosecutor said. “He was attempting to hide from the federal authorities where all this money was coming from and why he was washing it through his accounts.”

The FBI first encountered the defendant in connection with a stolen IRS check that he cashed. Additionally, his name repeatedly surfaced during pro-active SAR searches by the local FBI office.

In fact, the defendant is the subject of numerous SARs filed since 2004. These records document a trail of fraudulent activity, including an incident where he attempted to cash a counterfeit check. Through periodic review of the SARs filed

for activity in the local area, the FBI also learned that the defendant was acting as a broker in a scheme to lure individuals to invest in a gold mine. In addition, several SARs include transactions related to the lottery scheme, including at least one SAR that documents the defendant's inquiries on how to avoid transactions that would trigger CTRs.

The investigation focused on a six-month period of frequent structuring related to the international lottery scheme. The FBI said the defendant "was going to great lengths to avoid the reporting requirements" of FinCEN during numerous transactions conducted between January and June 2006 at his bank.

The investigating agent said that the SARs were extremely helpful to the case and as noted, he could not have made the case without them. In addition to describing the suspect transaction, the SARs provided details about accounts, contacts, and phone numbers.

(Investigating Agency: Federal Bureau of Investigation)

CREDIT UNION FILES SUSPICIOUS ACTIVITY REPORT AND HELPS LAUNCH BANK FRAUD, INTERNATIONAL PAYMENT TRANSFERS INVESTIGATION

A federal credit union filed a SAR and helped initiate an investigation into a counterfeit check scheme that had similarities with Nigerian 419 fraud schemes. These frauds, designated as such because of the section of the Nigerian criminal code that prohibits them, often promise substantial payments to individuals who help a "victim" recover funds that are being held improperly. The defendant in this case cashed a series of counterfeit checks and wire transferred the proceeds to Nigeria. In addition, at about the time of the SAR filing, the defendant began making large cash deposits in amounts that appear to have been structured.

Two years later, a financial institution filed several SARs on the defendant documenting additional wire transfers to Nigeria. The information recounted in the SARs supports the charges prosecutors made that the defendant was part of a long-running scheme to defraud financial institutions. Prosecutors showed that he repeatedly attempted to cash counterfeit checks in the area despite warnings from authorities to stop.

The local United States attorney's office announced this year that the defendant pleaded guilty in federal court to one count each of bank fraud and engaging in monetary transactions in criminally derived property.

In connection with the guilty plea, prosecutors advised the court that the defendant engaged in a scheme to defraud a number of financial institutions by passing and attempting to pass counterfeit corporate checks. According to the U.S. attorney's office, the defendant would deposit the checks and then arrange to immediately withdraw money and, in some instances, wire it to contacts in Nigeria. He obtained further funds by depositing a series of 23 counterfeit

money orders into various branches of the credit union and then withdrawing the funds before the counterfeit nature of the instruments could be discovered. The indictment alleges that he fraudulently obtained approximately \$190,000 as a result of his actions.

“This case involves fraudulent bank transfers to Nigeria and money laundering,” said an IRS supervisory special agent, who also cautioned that private individuals, in addition to the banking industry, should be on guard to avoid entanglement in similar schemes.

The law provides for a total sentence of 30 years in prison for bank fraud and 10 years in prison for engaging in monetary transactions in criminally derived property, a fine of \$1,000,000 on the bank fraud charge and \$250,000 on the latter charge, or both. Under the Federal Sentencing Guidelines, the actual sentence imposed is based upon the seriousness of the offenses and the criminal history, if any, of the defendant.

(Investigating Agency: Federal Bureau of Investigation)

SUSPICIOUS ACTIVITY REPORT INITIATES INVESTIGATIONS INTO FRAUD, HIGH-YIELD INVESTMENT SCHEMES; EGMONT EXCHANGES LEAD TO FOREIGN ACCOUNTS AND ASSET SEIZURES

An FBI agent proactively reviewing SARs identified a potential fraud scheme. However, as he dug deeper into the scheme, he learned the perpetrators of the crimes were in fact victims of yet another fraud based on high-yield investments. This second scheme led to a series of international transactions in accounts that investigators identified through Egmont cooperation. The Egmont Group is an international coordinating body for financial intelligence units (FIUs) formed to promote and enhance international cooperation in anti-money laundering and counter-terrorist financing.

The unique Egmont channel was used to quickly exchange information with counterpart FIUs in other countries. The owners of the identified business were in fact operating a Ponzi scheme – promising investors huge returns that were in reality payments from newer investors in the scheme. When the owners needed cash to pay investors, they turned to the defendant who was operating his own fraud scheme

This year, separate United States Attorney’s offices announced that the defendant pled guilty to Conspiracy to Commit Wire Fraud and Tax Evasion. He faces up to fifteen years in prison, a \$750,000 fine, and will be ordered to pay restitution to his victims.

The charges stem from an investigation into the defendant’s participation in an international investment scheme wherein he promoted a high-yield investment opportunity in which he claimed he could obtain investors a 1,200% rate of return within six months. He told investors that he would generate these

returns by using investment money to “lease funds” which would be used in a high-yield trading program. For several years, the defendant, through an investment business, received over \$13 million from investors who thought they were leasing larger amounts of money to be used in high-yield trading programs as the defendant had promised. As part of the scheme, he sent the victims bank documents, supposedly issued by a legitimate bank, making it appear that he had accessed large amounts of money on their behalf as part of his leased funds program.

Believing they were leasing hundreds of millions of dollars to be used in high-yield investment programs, investors transferred over \$13 million to accounts controlled by the defendant, including accounts in Switzerland and the Bahamas. In reality, the bank documents sent by him were forged and his leased funds program did not exist. Instead of using the funds for their intended purpose, the defendant diverted investor funds for his own benefit, acquiring an airplane, yacht, and a new Mercedes Benz automobile. Furthermore, he failed to file U.S. Income Tax returns reporting the income he had made from the scheme.

Authorities in Switzerland and the Bahamas, working cooperatively with the Federal Bureau of Investigation, froze the defendant’s bank accounts, and eventually transferred the funds to the United States. In total, over \$5 million was repatriated to the United States from the Swiss and Bahamian bank accounts.

The FBI obtained seizure warrants and seized the airplane and automobile purchased by the defendant. He was arrested in 2005 and remains incarcerated pending his sentencing.

Investigators used BSA records extensively in this investigation. In addition to the SAR that initiated the case, banks and casinos also filed numerous BSA records on the defendant. Several SARs report transactions that are common in fraud schemes such as inbound wires into business accounts and payments made for such things as personal items and utilities. In addition, the SARs reference accounts in foreign countries. Several casinos filed CTRs on the defendant for large transactions, and one filed a SAR when he refused to provide his Social Security Number necessary for the completion of the CTR. Finally, a bank filed a SAR after the investigating agent contacted the bank about the defendant’s (fraudulent) account statements. In the SAR, the filing institution noted that his documents had actual bank officials’ names on them and were “very similar” to their own documents.

(Investigating Agency: Federal Bureau of Investigation)

Section 4 – Issues & Guidance

As we have done in previous issues, FinCEN has reviewed recent calls received on its Regulatory Helpline⁹ for the most frequently asked questions about suspicious activity reporting. In response to ongoing questions regarding definitions underlying suspicious activity categories, we are re-printing a piece previously published in SAR Activity Review 7.

In addition, we are taking this opportunity to highlight the recently released “Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting.” This publication is a compilation of useful information which FinCEN has discovered through its analysis of Money Services Business (MSB) SARs but should also be informative to other financial institutions. It provides tips for avoiding common mistakes and suggestions for establishing more efficient and effective anti-money laundering programs.

http://www.fincen.gov/SAR_Common_Errors_Web_Posting.pdf

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

In response to requests for an explanation or definition of the various characterizations of suspicious activity appearing in Item 35 of the depository institution Suspicious Activity Report form (Form TD F 90-22.47), FinCEN, with the assistance of members of the Bank Secrecy Act Advisory Group² SAR Feedback Subcommittee, prepared the table appearing on the following pages, which provides a listing of each category, certain Federal criminal statutes associated with the violation, and its explanation or definition. Please note that filers may select more than one type of characterization, if applicable, when completing the Suspicious Activity Report form. For example, Category C - Check Fraud and Category D - Check Kiting may be marked, or Category C - Check Fraud and Category H - Counterfeit Check may be marked.

⁹ FinCEN’s Regulatory Helpline (800-949-2732) is the primary means for the financial community to obtain regulatory guidance and answers to specific questions relating to the Bank Secrecy Act.

¹⁰ The Bank Secrecy Act Advisory Group is a task force established by Congress to coordinate Bank Secrecy Act-related matters. The Bank Secrecy Act Advisory Group is comprised of high-level representatives from financial institutions, federal law enforcement agencies, regulatory authorities and others from the private and public sector.

Violation Category	Characterization of Suspicious Activity The Reportable Conditions	Possible Federal Criminal Statute(s)	Explanation/Description
a	Bank Secrecy Act /Structuring/ Money Laundering	<p>31 U.S.C. Section 5311 and 31 C.F.R. Part 103 Bank Secrecy Act</p> <p>31 U.S.C. Section 5324 - Structuring Transactions to Evade Reporting</p> <p>18 U.S.C. Section 1956 - Laundering of Monetary Instruments</p> <p>18 U.S.C. Section 1957 - Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity</p>	<p>i. The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction recordkeeping and reporting requirement under federal law and reporting requirements under federal law</p> <p>ii. The transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or</p> <p>iii. The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts including the background and possible purpose of the transaction.</p> <p>There are four types of structuring activities that are reportable:</p> <ol style="list-style-type: none"> 1. To avoid generating any Currency Transaction Report, Form 8300 and supporting records, and to avoid any recordkeeping connected to monetary instruments. 2. To avoid the identification requirements, e.g. connected with non-bank money transmissions and purchase of monetary instruments. 3. To avoid suspicious detection and conventional monitoring thresholds and filters. 4. To avoid enhanced scrutiny or additional review frequently triggered by higher transaction amounts and thresholds. <p>Note: 18 USC 1956 creates 3 basic categories of Money Laundering:</p> <ol style="list-style-type: none"> 1. Conducting/attempting to conduct one or more financial transactions with proceeds from specified unlawful activity; 2. Transporting/transmitting/transferring one or more monetary instruments or funds into or out of the United States with intent to promote carrying out of unlawful activity, to conceal or disguise the proceeds of specified unlawful activity, or to avoid a state or federal transaction reporting requirement; 3. Where property has been represented to be from specified unlawful activity (to cover law enforcement-related sting operations where the property is really clean.) <p>See an expanded explanation of money laundering in Section 6 of this Issue.</p>

b	Bribery / Gratuity	18 U.S.C. Section 215 - Bank Bribery	Anyone who, in connection with bank business, corruptly gives, offers or promises anything of value to a bank official with the intent to influence or reward that official.
c	Check Fraud	18 U.S.C. Section 1344 - Bank Fraud	-This type of fraud takes on many forms including: altered checks; check kiting; charge-back check fraud; closed account fraud; and variations on check forgeries. Other common check fraud violations noted are the withdrawal of funds against checks with forged endorsements or maker's signatures and counterfeit checks.
d	Check Kiting	18 U.S.C. Section 1344 - Bank Fraud 18 U.S.C. Section 656/657 - Embezzlement, Theft or Misapplication of Funds	A practice in which an individual with accounts at two or more financial institutions intentionally utilizes the delay in the check clearing process to write checks from one account to deposit into the second account, all the while knowing that the first account does not have collected funds. The subject continues this cycle, moving checks between accounts, to make it appear as if funds are available and using the balance in the accounts for expenditures.
e	Commercial Loan Fraud	18 U.S.C. Section 1344 - Bank Fraud 18 U.S.C. Section 656/657 - Embezzlement, Theft or Misapplication of Funds	A fraudulent loan involving a corporation, commercial enterprise, or other type of business, usually secured by some form of collateral. One example includes banks advancing loan funds to car dealers via floor plan lines of credit secured by the automobiles in inventory. Collateral is later sold, out of trust, and proceeds are not applied to the loan thus creating a loss to the lender.
f	Computer Intrusion	18 U.S.C. Section 1030 - Computer Fraud	A person who gains access to a computer system of a financial institution to: * Remove, steal, procure or otherwise affect funds of the institution or the institution's customers * Remove, steal, procure or otherwise affect critical information of the institution including customer account information; or * Damage, disable or otherwise affect critical systems of the institution. Note: Does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information See Issue 3, page 15, of The SAR Activity Review for additional information on Computer Intrusion at the following hyperlink: http://www.fincen.gov/sarreviewissue3.pdf .
g	Consumer Loan Fraud	18 U.S.C. Section 1344 - Bank Fraud 18 U.S.C. Section 656/657 - Embezzlement, Theft or Misapplication of Funds	A loan extended to an individual for personal or household use that is obtained fraudulently. Incidents of consumer loan fraud primarily involve the submission of false .or forged statements by loan applicants.

h	Counterfeit Check	18 U.S.C. Section 1344 - Bank Fraud	A legitimate check that is altered or forged by hand or through the use of a computer or electronic/digital device that is compromised or scanned into a computer. The payee's name, dollar amount, check serial number, and date are changed though other data (including the authorized signature) remain as they appear on the original check. The counterfeit check is purported to be genuine and negotiated.
I	Counterfeit Credit/Debit Card	18 U.S.C. Section 1029 - Fraud and Related Activity in Connection with Access Device 18 U.S.C. Section 1344 - Bank Fraud	A person who knowingly commits fraud by producing, using, or selling one or more counterfeit credit or debit cards. A counterfeit or fake card is created through technology to emboss stolen or fictitious card numbers, along with hologram and card issuer images, and magnetic stripes on white plastic. The cards are used for fraudulent purchases or sold to other criminals for their use.
j	Counterfeit Instrument	18 U.S.C. Section 1344 - Bank Fraud	The manufacture, copy, reproduction, or forgery of an instrument with the intent to defraud a financial institution. Instruments could include notes, checks, securities, bonds, certificates and other negotiable financial instruments.
k	Credit Card Fraud	18 U.S.C. Section 1344' - Bank Fraud	The intentional procurement of goods, services or money, without the authorization of the; cardholder, credit card member or its agent, by using a stolen, lost, or cancelled credit card. May include Illegal purchases made in person, via the Internet or telephone, or through cash advances.
I	Debit Card Fraud	18 U.S.C. Section 1344 - Bank Fraud	The unauthorized use of a stolen, lost, or cancelled debit card for payment of goods or to acquire services or money. Debit cards are used in place of checks or cash and usually are tied to a checking account. Fraudulent use of the debit card depletes available funds in that account causing a loss to the bank customer or to the bank.
m	Defalcation/Embezzlement	18 U.S.C. Section 656/657 - Theft, Embezzlement, or misapplication of funds	A person who, for unauthorized personal use, embezzles, abstracts, purloins or willfully misapplies any of the moneys, funds or credits of a bank, branch, agency or organization or holding company or any moneys, funds, assets or, securities entrusted to the custody or care of such bank, branch, agency, organization, or holding company.

n	False Statement	<p>18 U.S.C. Section 1001 - False Statements or entries</p> <p>18 U.S.C. Section 1005 - False Entries</p> <p>18 U.S.C. Section 1014 - False Statements on a Loan or Credit Application</p>	<p>A person who knowingly and willfully commits one of the following:</p> <ol style="list-style-type: none"> 1. Falsifies, conceals or covers up by any trick, scheme or device, a material fact; 2. Makes any materially false, fictitious or fraudulent statement or representation; or 3. Makes or uses any false writing or document knowing the same to contain any materially false, fictitious or fraudulent statement or entry. <p>The false statement must occur in a matter within the jurisdiction of a branch of the United States Government; essentially, making a false statement to a government agency when it is carrying out its mission.</p> <p>Section covers oral or written false statements or misrepresentations made knowingly on a loan or credit application to an insured bank (e.g., willful overvaluing of land, property, securities, or other assets or the understatement of liabilities). Such statements or misrepresentations must have been capable of influencing the bank's credit decision. Actual damage or reliance on such information is not an essential element of the offense. The statute applies to credit renewals, continuations, extensions or deferments and includes willful omissions as well as affirmative false statements. Obsolete information in the original loan application is not covered unless the applicant reaffirms the information in connection with a renewal request. The application will trigger the statute even if the loan is not made.</p>
o	Misuse of Position I Self Dealing	<p>18 U.S.C. Section 656/657- Theft, Embezzlement, or Misapplication of Funds</p> <p>18 U.S.C. Section 644 - Banker Receiving Unauthorized Deposit of Public Money</p> <p>18 U.S.C. Section 215 - Bank Bribery</p>	<p>A person, who is not an authorized depository of public moneys, who knowingly receives from any disbursing officer, collector of internal revenue, or other agent of the United States, public money on deposit, or by way of a loan or accommodation, with or without interest, or otherwise than in payment of a debt against the United States, or uses, transfers, converts, appropriates, or applies any portion of the public money for any purpose not prescribed by law.</p>
p	Mortgage Loan Fraud	<p>18 U.S.C. Section 1344- Bank Fraud</p> <p>18 U.S.C. Section 656/657- Theft, Embezzlement, or Misapplication of Funds</p>	<p>A person who fraudulently obtains a mortgage for property or other asset primarily by the submission of false or forged statements on loan applications.</p>
q	Mysterious Disappearance	<p>18 U.S.C. Section 656/657 - Theft, Embezzlement, or Misapplication of funds</p>	<p>Unexplained disappearance of moneys, or other instruments of value, in bearer form, from a financial institution's branch, agency, organization, or holding company.</p>

r	Wire Transfer Fraud	18 U.S.C. Section 1956 - Laundering of Monetary Instruments 18 U.S.C. Section 1343 - Fraud by Wire, Radio or Television	A person who, intending to defraud or obtain money or property by fraudulent means of false pretenses, representations or promises, transmits an electronic funds transfer.
s	Other		A category used to report suspicious activity that does not fit into any other violations characterization.
t	Terrorist Financing	18 U.S.C. 2339(a) and 18 U.S.C. 2339(b) - Harboring and Concealing Terrorists	Persons or entities who provide material support or resources to various enumerated terrorist acts, including concealing or disguising the nature, location, source or ownership of the material support or resources. Also, persons or entities providing material support or resources to designated foreign terrorist organizations, or attempting or conspiring to do so. The statute explicitly provides for extraterritorial jurisdiction, meaning it can be applied to actions occurring outside the United States.
u	Identity Theft	18 U.S.C. Section 1028 - Identity Theft	A person who knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under applicable state or local law. See Issue 2, page 14 of The SAR Activity Review for further details about identity theft at the following hyperlink: http://www.fincen.gov/sarreview2issue4web.pdf

Section 5 – Industry Forum

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

Suspicious Activity Reporting Issues Confronting the Money Services Business Industry

By George R. Brown V

**Merle, Brown & Nakamura, P.C. for the
National Money Transmitters Association**

Money service businesses have been required to file SARs for over five years now. Even before this requirement, many MSBs were already filing SARs on a voluntary basis. Money transmitters are a large subset of MSBs that are heavily regulated on both the state and federal levels.

Due to the nature of this business and the lack of federal licensing requirements, onerous and detailed state regulations have developed that require money transmitters to obtain state issued licenses before they are permitted to engage in business in a state. Almost every state has such a licensing requirement. In this state licensing process, the money transmitters are almost always required to demonstrate, among many other things, a compliance program that ensures SAR filings will be made when required and all other federal compliance issues are addressed.

One method of engaging in business as a money transmitter is to become an authorized representative of another money transmitter. Basically, an authorized representative sells another money transmitter's product (money transfer services) on behalf of the other money transmitter. In most cases, the authorized representative does not have a license and is specifically permitted by state law to engage in business as a money transmitter without a license because they are acting as an authorized representative of another money transmitter who in fact possesses the required state licensing. When a licensed money transmitter engages in business through authorized representatives, the licensee is required to demonstrate to the state licensing authorities that the authorized representatives are fully integrated into the money transmitter's SAR compliance program and are independently meeting their SAR compliance requirements as well.

Unlicensed money transmitters (businesses engaged in the money transmission business without a license where such licensing is required and without having established a valid authorized representative relationship) face no such requirements from state level regulators and are a significant SAR compliance risk. Unlicensed money transmitters face none of the state licensing barriers to entering business. Unlicensed money transmitters are a substantial compliance risk to our financial system and our society in general.

Certainly, within the wide array of licensed money transmitters there are varying degrees of SAR compliance risk. But the fact that a money transmitter possesses a state issued license is a significant indicator of reduced compliance risk.

Different types of state-licensed money transmitters face different types of SAR compliance issues. Medium-to-large state licensed money transmitters have sophisticated software compliance systems used to detect patterns of suspicious activity in their enormous databases of transmission-related information. These are almost exclusively back office systems as the medium to large state licensed money transmitters have very little face-to-face contact with customers. The customer interaction is almost exclusively conducted by the authorized representative of the licensed money transmitter. Accordingly, it is entirely appropriate and expected that the authorized representative will be required to, and will, file SARs concerning suspicious activity that is apparent due to the particularities of any specific transaction.

Authorized representatives are often not engaged in money transmission as their main line of business, so they will not usually be as sophisticated as the licensed money transmitter which they represent. This lack of sophistication will not stop them from recognizing suspicious activity in the interaction with the customer. Suspicious activity that occurs in the actual transaction is largely obvious and apparent.

Smaller state-licensed money transmitters face a different set of problems. They are often burdened with detecting both the face-to-face related suspicious activity and the more nuanced suspicious activity detectable through transaction review after the face-to-face customer exchange is concluded. After a certain level of volume is achieved, back office suspicious activity detection will be very difficult without either a sophisticated compliance software system or substantial resources to devote to the project. This is a significant problem for small money transmitters as the cost and difficulty of obtaining and maintaining a compliance software system may be too great for their business to bear. This would be a fair issue for a bank or state or federal regulator to focus on in reviewing a small licensed money transmitter's business. Is its SAR compliance system sufficient given the volume of money transmissions it conducts?

Language and cultural concerns are another set of issues that affect a money transmitter's SAR compliance. Small-to-medium sized money transmitters' businesses, and authorized delegates of large money transmitters, are often

largely oriented towards various ethnic communities within the United States that are sending money to friends, businesses, and family members back in their home countries. These ethnic orientations permeate the entire money transmission business and result in customers, employees, officers, and owners being largely from the ethnic community served by the particular money transmitter. English is either a second language or not spoken at all in most circumstances. This does not stop the state-licensed money transmitter's SAR compliance. But the language barrier can make the compliance more difficult to achieve since translation can become a cost and a burden. Cultural issues are also a concern. Many of these ethnic communities are from cultures that instill a fear of government and third parties being involved in personal finances and families. This fear and mistrust can create misperceptions and misunderstandings. The ethnic oriented money transmitters are faced with a particularly difficult task of discerning between normal fear and mistrust and customers or other persons with more nefarious purposes or intents. One way of alleviating some of this problem would be to conduct community outreach in the specific languages involved and to provide SAR forms and compliance materials in the specific languages as well.

This brings up the issue of defensive SAR filings. Out of fear of punishment for failing to file an SAR when required, some have come to believe that it is better to err on the side of caution and file an SAR in much less clear circumstances than others. This deters the law enforcement value of SARs in general as it will result in many filings where there is no actual illegal activity even though an SAR may be called for because there is some aspect of the transaction creating suspicion and causing the need for a filing. Money transmitters know and take pride in knowing they are assisting law enforcement when filing SARs. A redesigned form could possibly allow the money transmitter to rate the transaction as to the level of suspiciousness. This would hopefully assist law enforcement in allocating resources appropriately.

For several years now, money transmitters have faced significant difficulties finding, obtaining, and keeping bank accounts that are necessary to keep their businesses efficient, profitable, and transparent. This problem affects all money transmitters, both large and small. Most in the industry have come to believe that the reason for the difficulties with bank relationships arise from a misperception that all money transmitters represent an unacceptable compliance risk for the bank.

This misperception is an unfair and unjust overgeneralization that fails to take into account the particular money transmitter involved. The most significant attribute that will distinguish a high risk money transmitter from a low risk money transmitter is whether the particular money transmitter in question is licensed by the state regulatory authorities where that money transmitter is engaged in business.

State-licensed money transmitters are well intentioned, highly regulated businesses that are well aware of their SAR compliance requirements and how those requirements affect their particular circumstances. Money transmitters are deeply indebted to FinCEN for their continuing commitment to the industry. Money transmitters look forward to new opportunities to work together in the future with FinCEN to create more useful SAR filings for law enforcement while possibly alleviating the banking crisis that has affected the industry.



Section 6 – 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

Money Services Business:

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

Casino or Card Club

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

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):

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)

- | | | | |
|--|--|---------------------------------------|--------------------------------------|
| <input type="checkbox"/> October 2000 | <input type="checkbox"/> June 2001 | <input type="checkbox"/> October 2001 | <input type="checkbox"/> August 2002 |
| <input type="checkbox"/> February 2003 | <input type="checkbox"/> November 2003 | <input type="checkbox"/> August 2004 | <input type="checkbox"/> April 2005 |
| <input type="checkbox"/> October 2005 | <input type="checkbox"/> May 2006 | | |

Please fax Feedback Forms to:

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

Appendix

Index of Topics from All Editions of *The SAR Activity Review - Trends, Tips & Issues*

Topic	Issue	Page	Hyperlink Address to SAR Activity Review Issue
Automated Teller Machine (ATM) Commonly Filed Violations	7	23	http://www.fincen.gov/sarreviewissue7.pdf
Automobile Retail Industry: SAR Analysis – Indications of Suspicious Activity	5	27	http://www.fincen.gov/sarreviewissue5.pdf
Boat/Yacht Retail Industry: SAR Analysis – Indications of Suspicious Activity	5	31	http://www.fincen.gov/sarreviewissues5.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
Convenience Checks	12	5	http://www.fincen.gov/sarreviewissue12.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
Credit Union Cooperatives	12	15	http://www.fincen.gov/sarreviewissue12.pdf
Detection of Unlicensed/Unregistered MSBs through SAR Filings	10	5	http://www.fincen.gov/sarreviewissue10.pdf
Detection of Unlicensed/Unregistered MSBs through SAR Filings – Pre & Post Guidance Comparison	11	6	http://www.fincen.gov/sarreviewissue11.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
Director's Forum: Issue 11	11	3	http://www.fincen.gov/sarreviewissue11.pdf
Director's Forum: Issue 12	12	3	http://www.fincen.gov/sarreviewissue12.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: Suspicious Activity Reporting Issues Confronting the Insurance Industry	11	45	http://www.fincen.gov/sarreviewissue11.pdf
Industry Forum: Suspicious Activity Reporting Issues Confronting the Money Services Industry	12	39	http://www.fincen.gov/sarreviewissue12.pdf
Industry Forum: USA PATRIOT Act's Full Weight Placed on Securities Firms	9	47	http://www.fincen.gov/sarreviewissue9.pdf
Insurance Industry – Suspicious Activity Report Filings	11	13	http://www.fincen.gov/sarreviewissue11.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: Debt Elimination Schemes	11	43	http://www.fincen.gov/sarreviewissue11.pdf
Issues and Guidance: Definitions and Criminal Statutes for SAR Characterizations	12	33	http://www.fincen.gov/sarreviewissue12.pdf
Issues and Guidance: Disclosure of SAR Documentation	2	36	http://www.fincen.gov/sarreview2issue4web.pdf

1	28	http://www.fincen.gov/sarreviewforweb.pdf
6	59	http://www.fincen.gov/sarreviewissue6.pdf
6	61	http://www.fincen.gov/sarreviewissue6.pdf
2	35	http://www.fincen.gov/sarreview2issue4web.pdf
2	35	http://www.fincen.gov/sarreview2issue4web.pdf
6	64	http://www.fincen.gov/sarreviewissue6.pdf
3	43	http://www.fincen.gov/sarreviewissue3.pdf
6	65	http://www.fincen.gov/sarreviewissue6.pdf
10	42	http://www.fincen.gov/sarreviewissue10.pdf
7	45	http://www.fincen.gov/sarreviewissue7.pdf
10	39	http://www.fincen.gov/sarreviewissue10.pdf
8	35	http://www.fincen.gov/sarreviewissue8.pdf
4	49	http://www.fincen.gov/sarreview082002.pdf
8	38	http://www.fincen.gov/sarreviewissue8.pdf
5	65	http://www.fincen.gov/sarreviewissue5.pdf
2	36	http://www.fincen.gov/sarreview2issue4web.pdf
9	43	http://www.fincen.gov/sarreviewissue9.pdf
12		http://www.fincen.gov/sarreviewissue12.pdf
1	27	http://www.fincen.gov/sarreviewforweb.pdf
4	50	http://www.fincen.gov/sarreview082002.pdf
7	47	http://www.fincen.gov/sarreviewissue7.pdf
5	66	http://www.fincen.gov/sarreviewissue5.pdf
8	41	http://www.fincen.gov/sarreviewissue8.pdf
11	39	http://www.fincen.gov/sarreviewissue11.pdf
1	27	http://www.fincen.gov/sarreviewforweb.pdf
5	66	http://www.fincen.gov/sarreviewissue5.pdf
10	44	http://www.fincen.gov/sarreviewissue10.pdf
7	30	http://www.fincen.gov/sarreviewissue7.pdf
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: Black Market Peso Exchange	11	28	https://www.fincen.gov/sarreviewissue11.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 Identifies Links in ATF Cases	11	34	http://www.fincen.gov/sarreviewissue11.pdf
Law Enforcement Case: BSA Data Instrumental in Drug Cases	11	34	http://www.fincen.gov/sarreviewissue11.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	12	22	http://www.fincen.gov/sarreviewissue12.pdf
Law Enforcement Case: Check Cashing Business	3	34	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Check Kiting	11	33	http://www.fincen.gov/sarreviewissue11.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 Elected Official	12	21	http://www.fincen.gov/sarreviewissue12.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: Embezzlement by Former Bank Executive	11	33	http://www.fincen.gov/sarreviewissue11.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: High-Yield Investment Schemes	12	30	http://www.fincen.gov/sarreviewissue12.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 Iran	11	27	http://www.fincen.gov/sarreviewissue11.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: Insider Fraud	11	33	http://www.fincen.gov/sarreviewissue11.pdf
Law Enforcement Case: Insurance Embezzlement Scheme	11	32	http://www.fincen.gov/sarreviewissue11.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 Lottery Scheme	12	28	http://www.fincen.gov/sarreviewissue12.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: Mortgage Elimination Scheme	11	31	http://www.fincen.gov/sarreviewissue11.pdf
Law Enforcement Case: Mortgage Fraud Scheme	12	26	http://www.fincen.gov/sarreviewissue12.pdf
Law Enforcement Case: Nigerian Advance Fee Scam	6	40	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Nigerian Payment Transfers Scheme	12	29	http://www.fincen.gov/sarreviewissue12.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: Organized Crime & Possible Terrorist Financing	12	23	http://www.fincen.gov/sarreviewissue12.pdf
Law Enforcement Case: Payroll Scheme with ties to Organized Crime	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: Racketeering Scheme in Trash Hauling Industry	11	30	http://www.fincen.gov/sarreviewissue11.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: Stored Value Cards	12	24	http://www.fincen.gov/sarreviewissue12.pdf
Law Enforcement Case: Structured Deposits Exceeding \$700,000	7	34	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Structured Deposits Totalling \$500,000	11	29	http://www.fincen.gov/sarreviewissue11.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 Automobile Dealership	12	25	http://www.fincen.gov/sarreviewissue12.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 Characterizations “Other”	12	12	http://www.fincen.gov/sarreviewissue12.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: Date to Use When Correcting Previously Filed SARs	11	37	http://www.fincen.gov/sarreviewissue11.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: Individual Tax Identification Numbers and Social Security Numbers	11	37	http://www.fincen.gov/sarreviewissue11.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 International Lottery Scams	11	35	http://www.fincen.gov/sarreviewissue11.pdf
SAR Tips: Suspicious Activity Reporting for Third Party Receiver of Funds Scams	10	36	http://www.fincen.gov/sarreviewissue10.pdf

SAR Tips: Special Guidance Related to Identify 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 09/11/2001 & 09/11/2001 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 – Update	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

