The SAR Activity Review

Trends Tips & Issues

Issue 18

Published under the auspices of the BSA Advisory Group.
October 2010

Financial Crimes Enforcement Network

The SAR Activity Review

Trends Tips & Issues

Issue 18

Published under the auspices of the BSA Advisory Group.
October 2010

Table of Contents

The SAR Activity Review **Index** is available on the FinCEN website at:
http://www.fincen.gov/news_room/rp/files/reg_sar_index.html
For your convenience, topics are indexed alphabetically by subject matter.

The **Archive of Law Enforcement Cases** published in *The SAR Activity Review* can be accessed through the following link:
http://www.fincen.gov/news_room/rp/sar_case_example.html

Introduction

The SAR Activity Review – Trends, Tips & Issues is a product of continuing dialogue and close collaboration among the nation's financial institutions, law enforcement officials, and regulatory agencies to provide meaningful information about the preparation, use, and value of Suspicious Activity Reports (SARs) and other Bank Secrecy Act (BSA) reports filed by financial institutions.

As this is a general edition of *The SAR Activity Review*, readers will note that the articles cover a wide range of topics. However, to the extent that there is a unifying theme, we feature several articles that aim to address some issues raised during the outreach initiative to depository institutions with assets under $5 billion that the Financial Crimes Enforcement Network (FinCEN) is continuing to conduct this year.

The *Trends & Analysis* section begins with an in-depth look by FinCEN's Office of Regulatory Analysis (ORA) at SARs filed by firms in the securities and futures industries on suspicious activity related to commercial real estate investment vehicles. Additionally, ORA offers an initial analysis of Suspicious Activity Reports by Depository Institutions (SAR-DIs) referencing debt relief and debt settlement. This section closes with an examination of inquiries received by FinCEN's Regulatory Helpline between July 1, 2009, and June 30, 2010.

Several of the success stories highlighted in the *Law Enforcement Cases* section are groundbreaking cases in the use of charging and in successful convictions. Of particular note, we discuss a conviction on structuring charges where there was no allegation that the funds were illegally derived.

In *Issues & Guidance*, we present an article on the value of BSA data that provides material that BSA Compliance Officers may consider adapting for use when addressing their Boards of Directors. We also spotlight the 314(b) information sharing program in our continued efforts to promote its use by industry. This article complements the *Industry Forum*, which provides an industry perspective on the 314(b) information sharing program and gives practical tips for seeking cooperation from other institutions with the information sharing process.

As always, we very much appreciate any feedback you can offer. Please take a moment to fill in the form in Section 6 to let us know if the topics we have covered are helpful to you, as well as what you would like to see covered in future editions. The form may be forwarded to FinCEN at the email address sar.review@fincen.gov.

We would also like to thank the members of the Bank Secrecy Act Advisory Group (BSAAG) SAR Activity Review Subcommittee, who assist in suggesting articles that would be useful to industry, as well as the Co-chairs noted below, who assist in shepherding this publication.

Lilly Thomas
Vice President and Regulatory Counsel
Independent Community Bankers of America

Helene Schroeder
Special Counsel
Commodity Futures Trading Commission

Please do not submit questions regarding suspicious activity reports to The SAR Activity Review mailbox.

Section 1 — Director's Forum

Welcome to the eighteenth edition of *The SAR Activity Review - Trends, Tips & Issues*. For ten years, at the direction of Congress, FinCEN has been providing this publication as a resource for the financial services industry. It has matured into a resource for the law enforcement and regulatory communities as well. FinCEN continues its efforts to demonstrate to the financial industry that Suspicious Activity Reports (SARs) are not just a supremely valuable resource for law enforcement and regulatory professionals, but also provide unique and valuable information for the businesses which provide them. In many ways, and in particular through the *Review*, we aim to demonstrate how SARs, when examined and analyzed in aggregate, can uncover trends, patterns, and schemes that may not be apparent on the local level, but become obvious when viewed across the national landscape.

Businesses can use this information to identify trends in fraud and money laundering that may affect their revenue, their customers, or their reputations. Compliance professionals are necessarily familiar with the rules, advisories, and analytical reports that FinCEN regularly produces, but can the same be said for a financial institution's managers and board members? As part of our outreach initiatives, FinCEN staff and I have visited many financial institutions of all sizes representing several different business lines subject to BSA/AML regulations. I have come to further understand the challenges many face in getting the appropriate resources and management attention to compliance issues. It is my hope to help by emphasizing that SARs, and the information they provide, are a vehicle for reciprocal benefits between the government and industry. That is an important point to remember as financial professionals dedicate considerable time to understanding the changing financial landscape brought about by reform legislation. BSA/AML compliance must remain at or near the top of any financial institution's list of priorities. The information that SARs provide protects customers, businesses, and the integrity of the financial system itself.

In this issue, we present a number of interesting articles that hew closely to that theme. Our analysis has uncovered important information concerning commercial real estate investment vehicles and how they may be misused for criminal gain. Also, we have looked into burgeoning trends in debt relief scams that may affect your business and your customers. The SARs that have been filed concerning those activities, while they report local activity, have national import and serve to protect your business from losses and your customers from predation.

The trend in typical calls to our Regulatory Helpline shows a growing maturity in BSA/AML compliance. It is important to remember that the BSA/AML regulatory scheme is still relatively young; SAR filing for depository institutions has only been in place since 1996, and more recently for other industries. Nevertheless, we can see from the types of calls we get that compliance professionals are becoming more comfortable with the technical aspects of filing and are focusing more on how to work more effectively with law enforcement to help catch criminals.

Again, to demonstrate the importance of reciprocal benefits, we present an *Industry Forum* article by Jeffrey Halperin of MetLife who explains and discusses the benefits of utilizing Section 314(b) authorities that were created under the USA PATRIOT Act.

Please make good use of and share our section on law enforcement case examples that truly bring home the value of the BSA data to catch criminals and protect us all. We also welcome your comments through our feedback form, and encourage readers to submit their ideas for future articles.

/s/

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

Section 2 - Trends & Analysis

This section of *The SAR Activity Review - Trends, Tips & Issues* contains an analysis of Suspicious Activity Reports (SARs) filed by firms in the securities and futures industries related to commercial real estate investment vehicles. Following this article we provide an analysis of Suspicious Activity Reports by Depository Institutions (SAR-DIs) whose narratives contain the terms "debt relief" and "debt settlement," as well as an analysis of inquiries received by FinCEN's Regulatory Helpline.

Commercial Real Estate Investment Vehicles

By FinCEN's Office of Regulatory Analysis

Background

Since 2006, FinCEN has published extensively on residential mortgage fraud as identified through Bank Secrecy Act (BSA) filings by depository institutions. It has also published reports on commercial real estate (CRE) fraud. This is FinCEN's first publication on investment vehicles in commercial real estate, with a focus on two types of investment vehicles: real estate investment trusts (REITs) and commercial mortgage backed securities (CMBS). This assessment aims to focus industry awareness on reported types of suspicious activity involving these investment vehicles.

Methodology

Analysts identified suspicious activity related to REITs and CMBS by searching for key words in the narrative, subject and instrument fields of SAR filings submitted by firms in the securities and futures industries[1] and depository institutions[2] prior to

1. Firms in the securities and futures industries use FinCEN Form 101 (SAR-SF).
2. Form TD F 90-22.47

March 31, 2010. Analysts searched for approximately 30 terms that are commonly associated with CRE instruments such as commercial mortgage backed securities, real estate investment trusts, and real estate trusts.

Working Definitions

Terminology related to commercial real estate investment products varies widely and is often unclear due to the complexity of the instruments. For purposes of this report, FinCEN used the following working definitions.

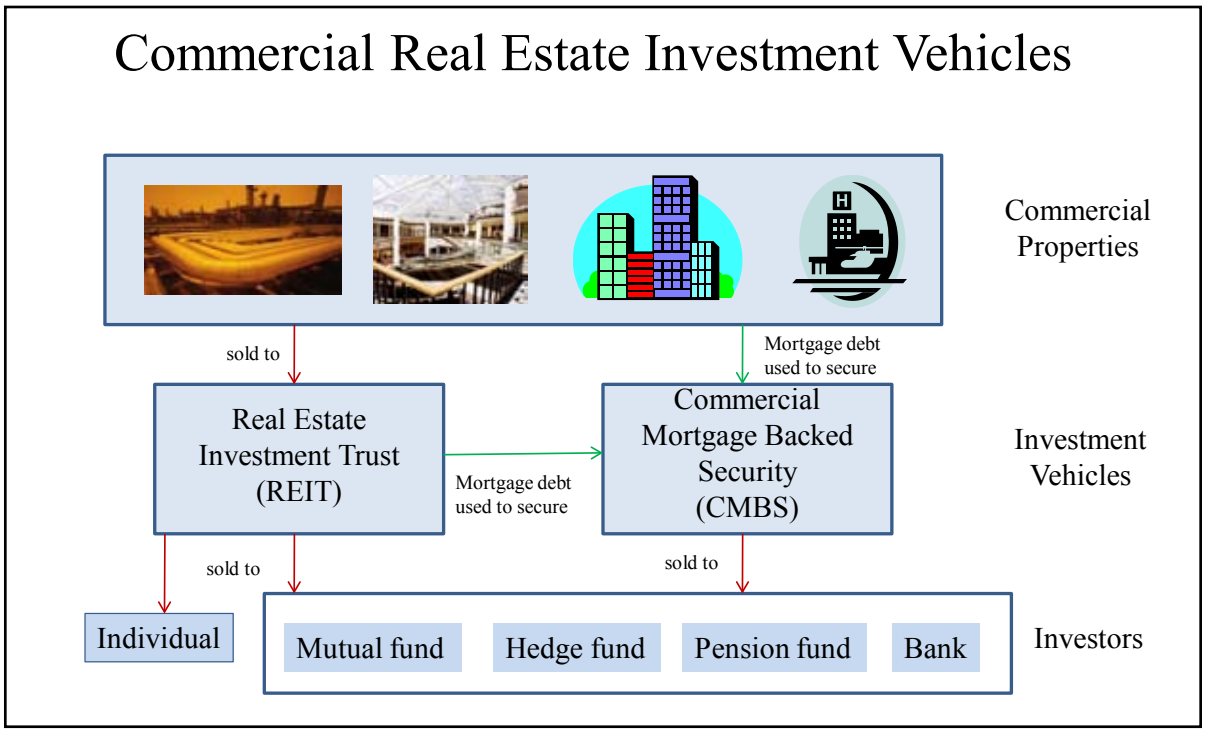
REITs[3], which came into formal existence in the 1960s due to tax law changes[4], are entities that typically own multiple commercial properties, often focused in one sector of the commercial real estate market. Institutional and individual investors can purchase REIT shares in the public market or in private offerings.

CMBS have existed since the mid-1990s.[5] According to the Congressional Oversight Panel, "CMBS are asset-backed bonds based on a group, or pool, of commercial real estate permanent mortgages. A single CMBS issue usually represents several hundred commercial mortgages, and the pool is diversified in many cases by including different types of properties. For example, a given CMBS may pool 50 office buildings, 50 retail properties, 50 hotels, and 50 multifamily housing developments." Some CMBS contain mortgages of REIT-owned properties. CMBS investors are primarily institutions purchasing in a quasi-public market.

Figure 1 illustrates how commercial properties are packaged into REITs and CMBS.

3. http://www.sec.gov/answers/reits.htm
4. Public Law 86-779, 74 Stat. 998 (Sept. 14, 1960), Part II – Real Estate Investment Trusts
5. The Congressional Oversight Panel was established in 2008 to provide legislative oversight of the Troubled Asset Relief Program. Congressional Oversight Panel February 10, 2010 report pp. 48-53 at http://cop.senate.gov/documents/cop-021110-report.pdf.

Figure 1: Commercial Real Estate Investment Vehicles



Significant Findings

"CMO" Most Common Filer Term for CMBS

Filers consistently described REITs in precise terms, typically using either "REIT" or "real estate investment trust." In contrast, filers referenced CMBS in broader terms also used to describe other investment vehicles.[6] Most commonly, filers characterized CMBS as "collateralized mortgage obligations" or "CMOs." As CMOs may refer to a range of instruments, and are not linked exclusively to commercial property, term searches alone did not suffice to identify reports involving CMBS. In SAR-SF reports, filers referenced 96 CMOs involving either CMBS or non-CMBS vehicles. By researching online industry sources, analysts obtained additional information on securities where filers specified a CUSIP number (SAR-SF, fields

6. The terms "CMBS" and "commercial mortgage backed security" appeared in only five SAR-SF filings and eight depository institution SAR filings. Filers characterized securities instruments either in narrative sections of SARs or in the instrument section of the SAR-SF (Part II, Field 23r).

24-29).[7] As seen in Table 1, only 26 percent of "CMO" references clearly involved a CMBS.[8] More CMO filings actually referenced residential mortgage backed securities (RMBS) than CMBS.

Table 1: Meaning of "CMO" in SAR-SF Filings

Meaning	*% filings*
RMBS	35%
Unable to determine	30%
CMBS	26%
Stock	4%
Other	3%
REIT	1%

In depository institution SARs, filers referenced "CMO" 125 times. However, only 14 percent of these references involved a mortgage security, as seen in Table 2.

Table 2: Meaning of "CMO" in Depository Institution SAR Filings

Meaning	*% filings*
Commercial money order	20%
CMO risk management	18%
Company name contains CMO	15%
CMO securities	14%
Cash management online	10%
Unable to determine	11%
Chief marketing officer	6%
Cash management officer	2%
Other	2%

7. A CUSIP is the identification number assigned to all stocks and registered bonds in the United States and Canada. The Committee on Uniform Securities Identification Procedures (CUSIP) oversees the entire CUSIP system.

8. Due to rounding, totals in Tables 1 and 2 do not add up to 100 percent.

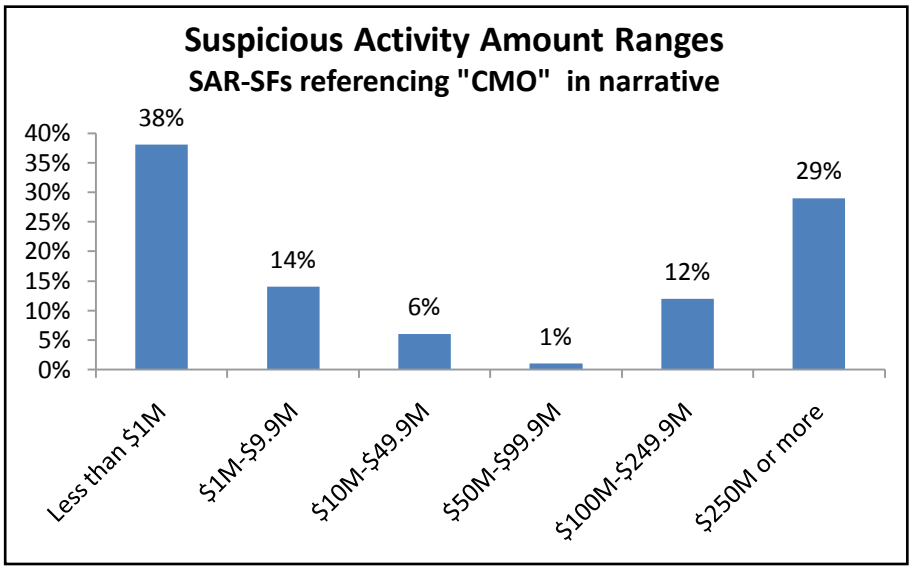
Highest Suspicious Activity Amounts in CMO-Related SAR-SFs

Suspicious activity amounts were significantly higher for SAR-SFs referencing CMOs than for other types of filings reviewed. The median suspicious activity amount in SAR-SFs referencing CMOs was $6 million, compared to low six figures for REIT-related filings and depository institution SARs referencing CMOs.

Table 3: REIT and CMO SAR Statistics		
	# Filings referencing narrative term (Median Suspicious Activity Amount)	
	SAR-SF	***SAR-DI***
REIT	56 ($209,500)	269 ($105,000)
CMO	94 ($6,000,000)	125 ($191,200)

Filers cited suspicious activity amounts of $250 million or more in over a quarter of SAR-SFs referencing CMO in the narrative.

Figure 2: CMO Suspicious Activity Amounts



Suspicious Activity Patterns

Suspicious activity patterns cited by filers also differed between CMO and REIT-related filings. In the majority of depository institution SARs related to REITs, filers cited suspected money laundering or structuring activity. CMO filings often had more complex activity patterns, which filers categorized as "other" and described in narratives.

Table 5: Suspicious Activity Types

Most Frequent Type			Second Most Frequent Type		
	SAR-SF	***SAR-DI***		***SAR-SF***	***SAR-DI***
REIT	Other (21%)	ML/structuring (57%)[9]	REIT	ML/structuring[10] (20%)	Check fraud (10%)
CMO	Other (28%)	ML/structuring (28%)	CMO	Securities fraud (22%)	Other (22%)

Valuation of Securities

Filers reported suspicious activity involving pricing disparities in 34 SAR-SFs, or 37 percent of SAR-SFs referencing CMOs. While the face values of the CMOs had not changed since issuance, their market values had greatly diminished, some reportedly to as little as 1 percent of face value. Filers reported many subjects who applied for loans based on the face value of the security. Other pricing issues included disputes with customers about the value of their mortgage securities, suspicious trading designed to impact market value, and reports of "offers" to purchase securities substantially above market value.

The remainder of this report focuses on suspicious activity patterns and examples found in SARs with activity amounts over $2 million, involving only CMBS or REITs, taking place between 2007 and 2010. These examples were primarily found among CMO-related SAR-SF filings but also included selected REIT-related filings.

9. This is an abbreviation for "BSA/Money laundering/Structuring" from Part 35a of TD F 90-22.47.
10. This is an abbreviation for "Money laundering/Structuring" from Part 30l (30L) of FinCEN Form 101.
11. Face value usually represents the amount invested in a bond (including CMBS) upon issuance. At any point in the future, the market value of a bond may be greater or less than face value, depending on the perceived risks associated with the bond.

Irregular Trading

Filers repeatedly cited subjects for unusual or inexplicable trading patterns. For instance, some subjects frequently traded CMBS, generated suspicious CMBS trading profits, charged fees for allowing CMBS to pass through their accounts, and may have offered unregistered securities or violated trading volume rules.[12]

Ponzi schemes and Investment Fraud

Filers reported several Ponzi schemes operating as REITs, commercial real estate securities funds, timeshares and other investment vehicles.

Misleading or False Information

Filers discovered misleading or false information provided by executives about bank investments in mortgage securities or by commercial mortgage customers.

Suspicious Activity Examples

CMBS Trading Network

Fourteen filers submitted approximately 30 SAR-SFs on a network of investors across the United States for suspicious trading activities involving several CMBS worth billions of dollars. Myriad pricing and trading issues were evident in these SARs. Suspicious activities included securities fraud (16 percent of reports), significant wire or other transactions without economic purpose (14 percent), pre-arranged or other non-competitive trading (11 percent), wash or fictitious trading (9 percent), embezzlement/theft (7 percent), money laundering/structuring (7 percent), suspicious documents or identification (5 percent), forgery (4 percent), and other (26 percent). Filers cited frequent movement of securities with face values in excess of $100 million and market values of under $1 million between accounts within this network, among other activities.

12. An unregistered securities offering is an offering of securities that is not registered with the Securities and Exchange Commission (SEC) under the Securities Act of 1933. The Securities Act of 1933 requires the registration of public offerings of securities through the filing of disclosure documents with the SEC. In addition, registration requirements may appear in the securities or "Blue Sky" laws of the States.

Ponzi Schemes – Real Estate Securities Hedge Fund and Private REIT

Several filers reported suspected Ponzi schemes where subjects gathered client funds for investment in commercial real estate or real estate securities without actually purchasing the underlying assets. A hedge fund claimed to invest millions in CMBS and credit derivatives, but the filer found no evidence of CMBS ownership. The hedge fund primarily bought long-term certificates of deposit earning minimal interest, which were inconsistent with the fund's investment strategy. In addition, the filer noted many small client deposits, consistent with a Ponzi scheme.

Filers submitted six SARs totaling $15 million on another suspected Ponzi scheme that purported to involve the management of a REIT. Operators of the scheme claimed that a U.S. based, privately owned REIT was investing in properties in a high risk foreign jurisdiction. One subject was a U.S. licensed stock broker who directed clients' retirement investments into the REIT. Filers reported that the U.S. subject lost his license and that foreign law enforcement criminally charged an overseas subject participating in the scheme.

Misleading/False Information - Bank Executive, Commercial Mortgage Holder, and CMBS Certificate Holder

Several filers cited subjects for providing misleading information about real estate securities or securitized commercial mortgages. One filer cited a former Chief Executive Officer (CEO) for failing to disclose investment risks in certain CDOs, CMOs and trust preferred securities. The CEO had managed the investment portfolio, supposedly with a "very high" rate of return, and received large bonus payments. Later, the filer determined the CEO had misled bank management about the risks. As the economy declined, the securities' revaluation resulted in large losses, leaving the bank in an unsound financial position.

In another example, a filer reported that a private company with multi-family real estate holdings throughout the country omitted information about a previous foreclosure on loan applications for newly acquired properties. The servicer of the securitized loans failed to disclose that it was a party to the past foreclosure. Foreclosure of the new loans triggered a dispute about liability among the filing bank, which had originated the new loans, the special servicer,[13] and a purchaser of the securitized loan product.

13. A special servicer "performs workouts or foreclosure of non-performing loans in a pool, an important part of asset management on behalf of the trust and the investor." http://www.mbaa.org/files/CREF/committees/AssetAdministration/WhitePaper-_Final_REGAB.pdf

Another filer reported that after several weeks of negotiation with a potential CMBS seller, it discovered the seller was not the true owner of the CMBS certificate. The filer determined that the subject had fraudulently obtained the certificate by delivering an affidavit or similar document, which another financial institution mistakenly processed.

Unusually Profitable CMBS Trading by Hedge Fund

One filer cited a hedge fund and several other sophisticated investors for unusually profitable trading in CMBS. It reported a series of CMBS trades by the hedge fund, each completed in a single day, with profits ranging from a small percentage to over 50 percent. The filer suspected pre-arranged or other non-competitive trading between subjects because there was no news to account for the dramatic price increases.

Conclusions & Recommendations

REITs, CMBS, and other commercial real estate investment vehicles have the potential for various kinds of manipulation and fraud. Filers whose business is involved with these investment vehicles should be cognizant of the potential risks for high-dollar losses through illicit activity and the attendant SAR reporting responsibilities. The examples in this article may help to illustrate the many variations in such activity.

NEXT STEPS

FinCEN will continue to monitor SARs related to commercial real estate investment vehicles and report findings in future publications. As warranted, analysts will also assess SAR data related to other types of CMOs, such as RMBS.

Analysis of Suspicious Activity Reports by Depository Institutions (SAR-DIs) Containing the Terms "Debt Relief" and "Debt Settlement"

By FinCEN's Office of Regulatory Analysis

FinCEN reviewed Suspicious Activity Reports by Depository Institutions (SAR-DIs) reporting companies suspected to be involved in fraudulent debt settlement/debt relief schemes. The rise in consumer debt has increased the number of for-profit debt settlement/relief companies but some have engaged in deceptive, abusive and fraudulent practices victimizing consumers and at times financial institutions. Some debt settlement companies have charged fees to enroll customers in deceptive programs or to settle debts but did not provide the services while others misappropriated settlement payments, operated without a license, or facilitated identify theft.[14] There are over 50 publicly-announced investigations and regulatory actions against abusive and/or fraudulent debt settlement companies nationwide. The regulation of the debt settlement industry varies from state to state but on October 27, a new Federal Trade Commission (FTC) rule will come into effect that will, among other provisions, "prohibit debt relief companies that sell debt relief services over the telephone from charging a fee before they settle or reduce a customer's credit card or other unstructured debt." Additional provisions already took effect on September 27.[15]

Depository institutions operating in the United States are becoming increasingly aware of fraudulent practices and the number of related depository institution Suspicious Activity Reports (SARs) has steadily increased. In 2006 only 2 SARs related to debt settlement activities were filed while 42 reports were filed during the first half of 2010. In total, from January 2006 through June 2010, financial institutions filed 115 SARs totaling $135 million related to fraudulent debt

14. The Government Accounting Office (GAO) report number 10-593T of April 22, 2010, Debt Settlement, Fraudulent, Abusive, and Deceptive Practices Pose Risk to Consumers highlights the industry's problems. The report is available at www.gao.gov or by toll-free calling 866-801-7077.

15. For further information, see the FTC's press release, "FTC Issues Final Rule to Protect Consumers in Credit Card Debt," available at www.ftc.gov.

settlement activities other than mortgage fraud. The reports identified Florida, California and New York as the top three subject states followed by Maryland, Illinois, Tennessee, Massachusetts and Kansas.[16]

Narratives reviewed indicated that transactions not commensurate with the nature of the business or intended purpose of the accounts, and derogatory information obtained on subjects, led to the filing of the SAR(s). In many cases, the financial institution filed because the account activity was consistent with the derogatory information. Some accounts reflected a high percentage of returned deposits involving unauthorized Automated Clearing House (ACH) debits while others displayed extensive wire transfer activity among several accounts. Various accounts appeared to indicate misappropriation of deposited funds since the funds were depleted through ATM withdrawals or debit card purchases towards personal use, which did not match the account business model. Further, narrative reviews shed light onto the scams and schemes perpetrated or attempted by the debt settlement companies against consumers and/or financial institutions including:

- Attorney debt elimination scheme: Citing the Fair Debt Collection Practices Act (FDCPA), attorneys allegedly representing credit card holders submitted letters to financial institutions demanding that the institutions cease communication with the accountholders, including phone calls to accountholders and communications that involved the transmittal of monthly statements, annual privacy notices, change in terms notices, and collection letters. The attorneys falsely told the customers that once the financial institutions received the demand letters the financial institutions could not pursue further collection efforts. Other purported attorneys signed up thousands of credit card debtors for debt management services by claiming they would provide legal services to cancel the debts for pennies on the dollar. The attorneys told consumers that they had audited their accounts and found numerous violations of the Fair Credit Billing Act and had taken the initiative to send notices to creditors disputing all charges. The attorneys further claimed that once the notices were issued to the creditors, the consumers did not have to repay the debts, and the creditors could not sue or take further actions against the consumers.

16. FinCEN retrieved SARs filed from January 2006 through June 2010 that referenced "debt settlement" or "debt relief" in the narrative, or listed as a characterization of suspicious activity "debt settlement" or "debt relief" under "Other" (Field 35s of the SAR form). FinCEN excluded SARs that listed "mortgage loan fraud" as a characterization of suspicious activity (Field 35p of the SAR form), regardless of whether "debt settlement" or "debt relief" also appeared in the narrative or as a characterization of suspicious activity. These search parameters returned a higher number of reports than 115, but review of the narratives eliminated reports not relevant to the scope of the study. FinCEN did not search for references to "debt elimination."

- Up-front fees: Debt settlement companies required consumers to pay an up-front fee to join a debt assistance program that would eliminate the debt for a fraction of the amount owed. Many offered to refund the fee if the customer did not save a specified amount of money. Some groups claiming to be non-profit organizations offered debt counseling services targeting consumers with poor credit histories to help them obtain loans and credit cards or settle debts. The groups pressured the consumers to pay an entitlement fee within a short period of time or risk being placed on a non-existent waiting list. The debt settlement companies collected the fees through ACH deposits into their accounts, but did not provide the services. In another case, a merchant who accepted a major credit card as payment victimized the credit card company and many of the credit card holders when it solicited offers of debt consolidation without the credit card holders' knowledge or authorization. Using its merchant account with the credit card company, the merchant charged fees ranging from $200 to $1,000 for the unsolicited debt consolidation services. The merchant further defrauded the credit card company and individuals when it submitted hundreds of new credit card applications, also without the knowledge or authorization of the applicants, and collected a referral fee from the company.

- Misappropriation of payments: Companies promised debt elimination but instead diverted consumers' payments for personal use or for legal fees to file meritless lawsuits challenging creditors that would give the appearance of assisting the customers.

- Use of Fraudulent Documents: Individuals sent fraudulent bonded promissory notes to a financial institution to relieve debts. Upon interview by the financial institution, the individuals stated to have paid a small sum to a debt relief agency that assured them it was secured with deposits held at the Federal Reserve Bank in New York.

- Promotion of Debt Fraud: Debt settlement companies advised consumers on how to avoid financial responsibility by concealing funds from creditors. Financial institutions noticed customers who suddenly began to deal in cash by cashing paychecks when they previously had direct deposit, withdrawing large cash amounts and allowing small amounts to keep accounts open. Upon inquiring as to the reason for the cash, the customers stated to be acting under the advice of a debt settlement agency to leave no records of the funds' existence.

SAR narratives also showed that activities related to debt settlement facilitated identify theft and wire transfer fraud. Employees of debt settlement companies sold personal information including Social Security Numbers, and crime rings claiming to be debt relief agencies contacted credit cardholders and obtained personal information and credit card account numbers. Wire transfer fraud occurred when an advanced fee-type scam victimized individuals who wired funds abroad in response to offers of debt relief grants.[17] The victims were instructed to wire funds to cover taxes and fees for the debt relief grant to be issued. In return, the victims received worthless checks that were returned unpaid upon deposit. Further, one SAR reported on the owner of a debt settlement agency who offered cash to personnel of a bank to buy customer information to develop potential clients.

Analysis of SAR Inquiries Received by FinCEN's Regulatory Helpline

By FinCEN's Office of Outreach Resources

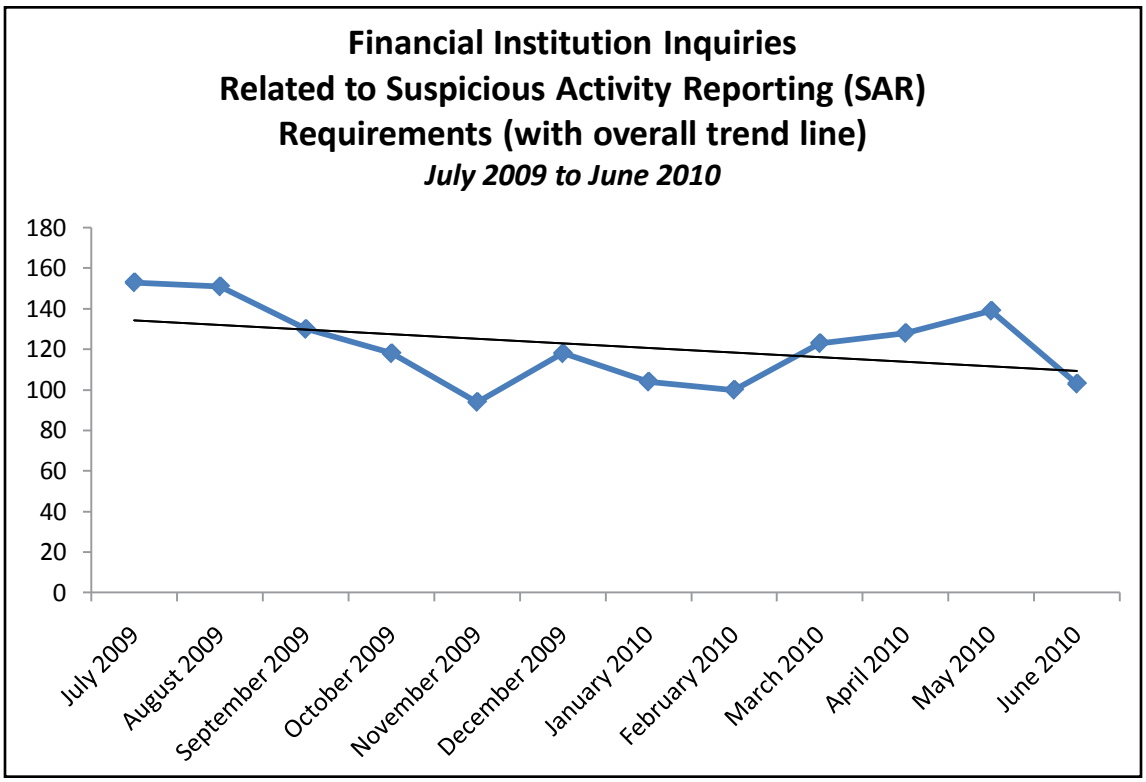
FinCEN operates a Regulatory Helpline that provides assistance for financial institutions seeking clarification of their obligations under the Bank Secrecy Act (BSA) and certain requirements under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act.[18] This article analyzes the 1,461 inquiries regarding suspicious activity reporting (SAR) requirements that the Regulatory Helpline received from July 1, 2009, through June 30, 2010.[19] This article also highlights helpful FinCEN guidance for the most frequently received inquiries, including guidance on filing SARs for ongoing or continuing activity and verification of a SAR filing. Finally, the article highlights the important topic of Remote Deposit Capture (RDC) services and the new Regulatory Helpline Hot Topics web page introduced last year.

17. For further information on advanced fee schemes generally, see the article "Advanced Fee Schemes" in *The SAR Activity Review – Trends, Tips & Issues*, Issue 4, page 49, http://www.fincen.gov/news_room/rp/files/sar_tti_04.pdf#page=55
18. Financial institutions can contact FinCEN's Regulatory Helpline at 800-949-2732.
19. All information provided in this publication has been aggregated to ensure the confidentiality of individual inquiries. The determination of entity type is primarily based upon caller self-identification.

Key Trends

Volume trends

During the twelve month period ending June 30, 2010, the Regulatory Helpline received 1,461 inquiries related to SAR requirements, or about 18 percent of all inquiries received. This was an 11 percent decrease in the number of SAR inquiries compared with the previous twelve month period ending June 20, 2009. The most noticeable decrease in SAR inquiries was related to "assistance with the SAR form," which decreased by 137 inquiries (22 percent). This was a key theme that was highlighted in the October 2009 SAR Activity Review and readers were provided multiple guidance pieces for informational purposes.[20] While "assistance with the SAR form" remains the most common type of inquiry, FinCEN welcomes the decrease in both the absolute and relative number of calls on this topic as a reflection of financial institutions' increased level of comfort with the technical aspects of filing. There were also decreases in the volume of the inquiries related to "guidance on whether to file a SAR," "definitions and other guidance," and "additional steps a financial institution should take,"[21] which were also addressed in last year's article.



20. See *SAR Activity Review, Trends Tips and Issues*, Issue 16 (http://www.fincen.gov/news_room/rp/files/sar_tti_16.pdf#page=30).

21. Financial institutions requested guidance on what steps they should take in addition to filing a SAR, such as closing an account or contacting local law enforcement.

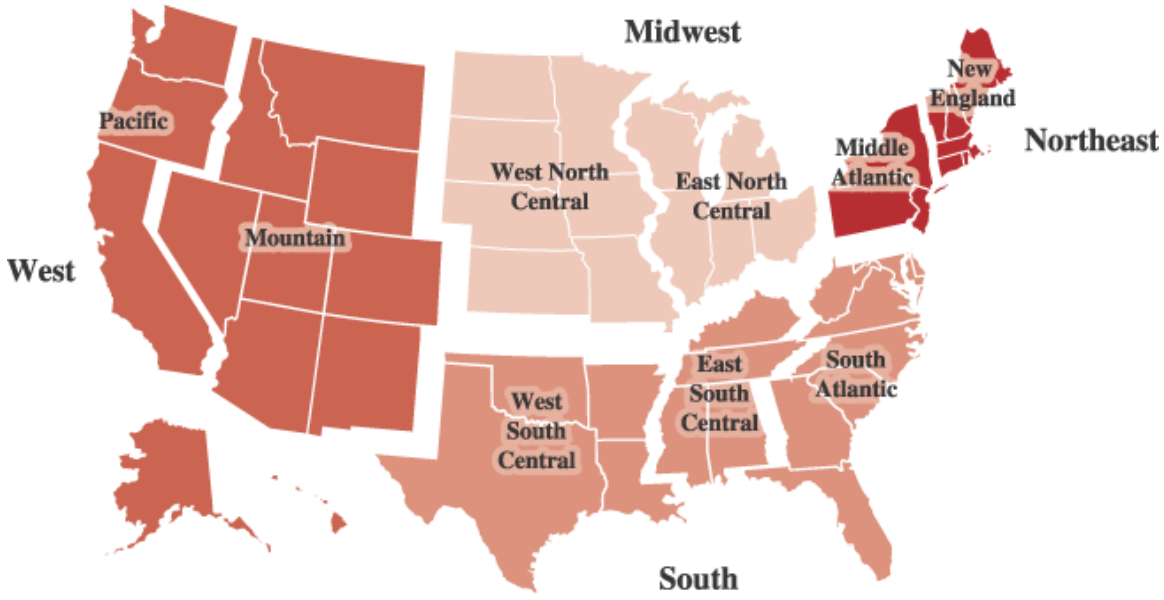
Geographic Trends

Inquiries were received from every state except Rhode Island, as well as from Puerto Rico, the District of Colombia, and Ontario, Canada. Ten states, primarily California, Texas, New York, Florida, and Illinois, accounted for half of all the inquiries from the study time period. As with the previous year's analysis, there remained consistent trends in the geographic dispersion of the inquiries, with the highest concentration again in the South.

There were some slight differences in the timing and type of institutions that contacted the Regulatory Helpline across the four main regions of the country. Most notably, credit unions accounted for 27 percent of all inquiries in the West Region, while averaging only 13 percent across the other three regions.

SAR Inquiries by Region

July 1, 2009 to June 30, 2010

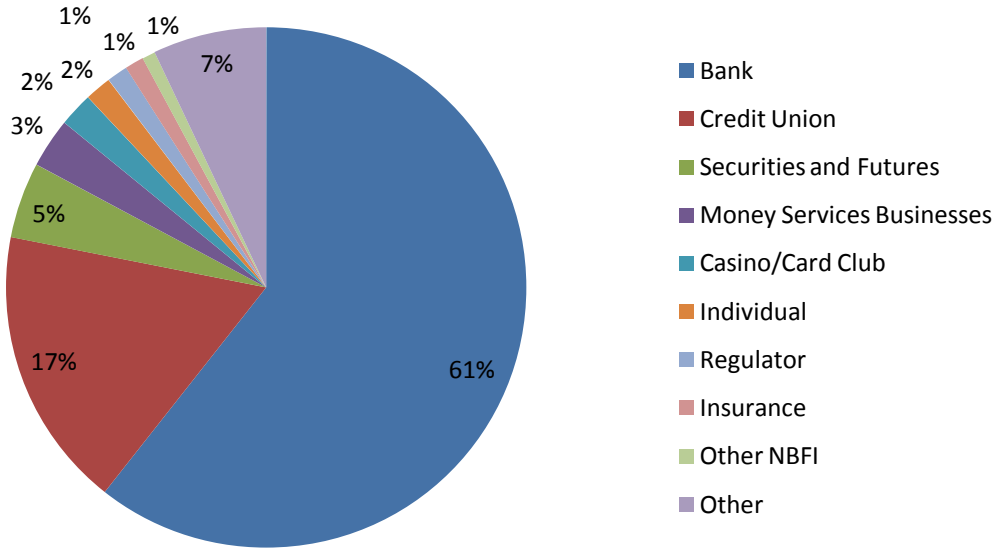


WEST = 286	**NORTHEAST = 296**
Pacific = 204	New England = 98
Mountain = 82	Middle Atlantic = 198
SOUTH = 499	**MIDWEST = 323**
West South Central = 190	West North Central = 128
East South Central = 58	East North Central = 195
South Atlantic = 251	
	All Other = 57

Institution Type Trends

SAR Inquiries by Type of Financial Institution

July 1, 2009 to June 30, 2010



Bank	886	Credit Union	255
Securities and Futures	69	Money Services Businesses[22]	45
Casino/card club	31	Individual	24
Regulator	19	Insurance	17
Other NBFIs and businesses[23]	11	Other	104
Total Requests	**1,461**		

22. This category includes money transmitters; currency dealers and exchangers; check cashers (who do not have a SAR filing obligation); issuers, sellers, and redeemers of traveler's checks, money orders, and stored value (transactions involving solely the issuance, sale, or redemption of stored value are not subject to the SAR filing obligation); and the United States Postal Service (for certain activities).

23. This category includes all other non-bank financial institutions and businesses, such as loan and finance companies, vehicle sales, and dealers of precious metals/jewelry.

Key Issues and Themes

Number and Types of Inquiries Received
July 1, 2009 - June 30, 2010

Assistance with SAR Form	**486**
SAR item instructions	322
Form corrections	71
SAR narrative	39
Aggregation	24
Filing deadline	20
Deletion or rescission of a filed SAR	10
Guidance on Whether to File a SAR	**306**
Whether to file a SAR	179
Regulation	59
Monetary thresholds	48
Guidance on attempted activity	20
SAR Sharing and Disclosure	**282**
Sharing - Law Enforcement	118
Other disclosure questions	91
Replying to a subpoena	46
Sharing - Regulators/Auditors	14
Sharing - Corporate Structure	13
SAR Filing on Continuing Activity	**101**
Aggregation	50
Frequency of SAR filings	27
Whether to file a SAR	13
FinCEN guidance	6
Monetary thresholds	5
Verification of SAR Filing	**79**
Verification of filing	51
Obtaining copies of a SAR	28
Characterizations of Suspicious Activity	**52**
Definitions	52
Additional Steps a Financial Institution Should Take	**39**
Notification of authority (e.g. FBI, DEA, etc.)	25
Guidance on whether to close an account	14
E-Filing	**21**
Miscellaneous	17
SAR item instructions	4
Other	**95**
Miscellaneous	52
FinCEN guidance	11
SAR Activity Review	11
Safe Harbor	10
Regulation	6
General Guidance	5
Total Inquiries for July 1, 2009 to June 30, 2010	**1461**

During the twelve month period that ended June 30, 2010, the most frequent types of inquiries received on the Regulatory Helpline remained the same as those highlighted in the October 2009 SAR Activity Review.[24] During this period, inquiries related to "assistance with SAR form" accounted for 33 percent of all SAR inquiries, compared with 38 percent of all SAR inquiries during the previous 12 month period. The following guidance provides helpful answers for many SAR form assistance questions: SAR Narrative Guidance Package Inquiries related to "guidance on whether to file a SAR" accounted for 21 percent of all SAR inquiries (21 percent for the previous 12 months); to assist in making this internal decision, institutions may refer to resources such as the FFIEC BSA/AML Examination Manual, Suspicious Activity Reporting Overview, SAR Decision-Making Process.[25]

Inquiries related to "SAR sharing and disclosure" accounted for 19 percent of all SAR inquiries (13 percent for the previous 12 months); to aid institutions in responding to law enforcement and regulatory authorities' requests for SAR information and supporting documentation, FinCEN issued guidance in June 2007 entitled, Suspicious Activity Report Supporting Documentation (FIN-2007-G003). Guidance on how to respond to a request for SAR information to support a civil case or when someone other than an appropriate law enforcement or supervisory authority makes the request is available in a previous SAR Activity Review (see The SAR Activity Review Issue 7 (August 2004), Section 4).

Highlighted below are more of the recent common inquiries to the Regulatory Helpline.

SAR Filing on Continuing Actvity

Institutions frequently seek the guidance of FinCEN's Regulatory Helpline with regards to filing SARs on continuing activity. There are several resources available that address these inquiries. In particular, banks should review the FFIEC BSA/AML Examination Manual, Suspicious Activity Reporting Overview, SAR Filing on Continuing Activity. The most common inquiries related to SAR filing on continuing activity were:

---

24. See *SAR Activity Review, Trends Tips and Issues*, Issue 16 (http://www.fincen.gov/news_room/rp/files/sar_tti_16.pdf#page=30).

25. Although the FFIEC Exam Manual is issued by the federal banking regulators regarding Anti-Money Laundering (AML) requirements applicable to banks, it contains guidance that may be of interest to other financial institutions.

1. How should we complete items 33 (Date or date range of suspicious activity) and 34 (Total dollar amount involved in known or suspicious activity) on the SAR form (referred to in the chart above as "aggregation")?

   Institutions can find guidance published in August 2002 by FinCEN in the SAR Activity Review Issue 4, Section 5 under the topic of "Filing a SAR For Ongoing or Supplemental Information."

2. How often should we file SARs for continuing activity?

   As a general rule, organizations should report continuing suspicious activity with a report being filed at least every 90 days. Guidance on this issue can be found in the October 2000 SAR Activity Review Issue 1, Section 5 under the topic of "Repeated SAR Filings on the Same Activity." Further guidance on this issue can be found in the April 2005 SAR Activity Review Issue 8, Section 4 under the FAQ "Correcting vs. Updating a Prior Report."

Special Topic

Remote Deposit Capture (RDC)

On March 17, 2010, FinCEN announced the assessment of a civil money penalty, in the amount of $110 million, against Wachovia Bank. The action represents the largest penalty action to date against a financial institution by FinCEN for violations of the Bank Secrecy Act (BSA), including a failure to apply systems and controls to manage the risk of money laundering within the bank's business lines, such as Remote Deposit Capture (RDC) from Mexico to the United States.

As this enforcement action highlights, financial institutions should fully understand and appropriately manage the risks associated with their RDC services, particularly those involving non-U.S. located customers. While FinCEN's Regulatory Helpline has received only a handful of inquiries regarding the application of BSA rules to RDC transactions, banks are strongly encouraged to review the RDC section of the FFIEC Examination Manual. This section highlights the potential risks and useful risk mitigation approaches for financial institutions to apply as part of providing their services. FinCEN will be further analyzing RDC and its risks and related SARs, and will be publishing updated information on this topic as appropriate and available.

Verification of SAR Filing

Institutions will occasionally contact the FinCEN Regulatory Helpline to verify the receipt, or request a copy, of a SAR filing. Financial institutions must maintain a copy of any SAR filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[26]

Due to the confidentiality of these reports, FinCEN is unable to verify the receipt of, or provide a copy of SAR filings. However, users of FinCEN's BSA E-Filing System[27] do receive receipt and acknowledgement of electronic files; and, as of September 12, 2009, FinCEN implemented SAR Acknowledgements for BSA E-Filing submissions. Institutions that utilize the BSA E-Filing system should keep in mind that they are still required to keep their SAR filings for five years, as they will not be able to retrieve filings from the BSA E-Filing System once they are submitted.

Regulatory Helpline Hot Topics

In October 2009, FinCEN created the Regulatory Helpline Hot Topics, which is located on the FinCEN homepage under "Most Requested." Regulatory Helpline staff identifies the most common recent inquiries from financial institutions on a regular basis and updates the hot topics webpage with links to the most useful related guidance. During the twelve month period that ended June 30, 2010, there were multiple hot topics related to SARs, including guidance on writing SAR narratives, responding to civil subpoenas for SARs, and responding to a law enforcement request for SARs. To see what your colleagues are contacting the Regulatory Helpline about, add the Regulatory Helpline Hot Topics to your favorite websites.

---

26. The record keeping requirement applies to each category of financial institution that has a requirement to file SARS: 31 CFR 103.15(c) [mutual funds]; 103.16(e) [insurance companies]; 103.17(d) [futures commission merchants and introducing brokers in commodities]; 103.18(d) [banks]; 103.19(d) [brokers or dealers in securities]; 103.20(c) [money services businesses]; and 103.21(d) [casinos].

27. http://bsaefiling.fincen.treas.gov/main.html

Section 3 - Law Enforcement Cases

This section of *The SAR Activity Review* affords law enforcement agencies the opportunity to summarize investigations where Bank Secrecy Act (BSA) information played an important role in the successful investigation and prosecution of criminal activity. This issue contains new case examples from federal and local law enforcement agencies. Additional law enforcement cases can be found on the FinCEN website under the link to Investigations Assisted by BSA Data. This site is updated periodically with new cases of interest, which are listed by the type of form used in the investigation, type of financial institution involved, and type of violation committed, and can serve as a valuable training tool.

Contributing editors: Shawn Braszo, Vanessa Morales, James Emery, and Jack Cunniff.

In this edition of *The SAR Activity Review*, we include some cases where defendants either pleaded guilty or were convicted at trial on BSA-related violations. We present these cases because prosecutors continue to see the value in using the BSA to combat a wide variety of criminal activity. For example, structuring can be shown with a bank statement disclosing numerous deposits of $9,900 made by an individual on consecutive days. Structuring with the intent of evading Currency Transaction Reports (CTRs) is in itself a Federal violation, with a penalty of up to 5 years imprisonment and a possible fine of $250,000. If the structuring involves more than $100,000 in a 12-month period or is performed while violating another Federal law, the penalty is increased to imprisonment not to exceed 10 years and/or a fine of $500,000.

We start with several cases where defendants conducted a pattern of structured transactions but the subsequent investigations did not produce a nexus to a criminal activity related to the source of the funds. In one case, the defendant chose a jury trial, where he was ultimately convicted of structuring. In another case, prosecutors used their discretion to charge the defendant with a misdemeanor. Federal authorities were able to bring money laundering charges in a case involving an Internet gambling ring where states would have been able to pursue only misdemeanor charges.

The BSA continues to play a role in drug cases. In a drug conspiracy case, prosecutors charged a defendant with structuring and money laundering rather than drug trafficking offenses. A second drug case describes how the defendant used nominees to hide assets. We also highlight several cases where BSA

information contributed to the prosecution of businesses and individuals. These cases involved commercial loan fraud, structured earnings and underreported income, and wire transfers to sanctioned countries.

Jury Convicts Defendant of Structuring, No Illicit Origin of Funds Alleged

A jury found the defendant guilty of structuring after a pattern of transactions designed to evade currency transaction reporting requirements was identified. Prosecutors did not allege that the structured funds were derived from criminal activity.

The jury found the defendant guilty of structuring based on two transactions he conducted on a single day. Over a period of weeks and using different bank branches, the defendant conducted transactions in amounts ranging from $5,000 to nearly $10,000. On one of the days during this period, the defendant deposited cash at one branch but withheld funds so that the institution would not file a CTR. He then deposited the funds into the account less than one hour later at a different branch.

The defendant refused to divulge the source of the structured funds. The defendant alternatively reported several occupations, including as the operator of a business with which the structured transactions were associated. The jury did not find the defendant guilty of the count charging structuring over several days, but did find him guilty of structuring the transactions that occurred on a single day.

Defendant Pleads Guilty in Structuring Case

A woman who continually conducted large cash transactions at casinos and structured those funds at her local bank pleaded guilty to a Title 12, Chapter 21 violation concerning record keeping requirements. Prosecutors charged her with a misdemeanor violation because they did not find any evidence of criminal wrongdoing associated with the origins of the currency. The judge sentenced the defendant to probation and a small assessment and fines. In addition, the defendant forfeited funds that had earlier been seized from her bank account.

Over a period of several months, the defendant made a series of structured deposits into her bank account with currency she received from a casino. In one instance, she received over $10,000 in currency from the casino and deposited the funds on multiple days over the next week. Several months later, she again received over $10,000 from the casino, and engaged in a similar series of deposits.

In addition, the defendant later used over $10,000 to purchase chips at the casino. On the same day, she received over $10,000 from the casino and made successive deposits into her bank account the following week. A number of months later, the defendant again received currency from the casino and engaged in a similar series of deposits. The pattern continued in the following weeks.

The defendant pleaded guilty to a misdemeanor charge under 12 U.S.C 1956.

BSA Records Identify Accounts and Transactions Related to an Illegal Gambling Enterprise

In a case where Federal prosecutors stepped in to help local law enforcement, BSA records identified millions of dollars generated through an illegal gambling operation. State authorities had few tools to punish the defendants because the state charges were only misdemeanors. To shut down the large operation, federal authorities brought charges, including money laundering, which could result in longer sentences.

The defendants were found guilty of conspiracy to operate an illegal gambling business, other charges related to the operation of an illegal gambling business, and money laundering. The defendants agreed to a forfeiture money judgment in the hundreds of thousands of dollars, as well as forfeiture of tens of thousands of dollars in bank accounts and several items of property.

The prosecution centered on a gambling enterprise that operated computerized gambling machines under the guise of internet businesses apparently unrelated to gaming. All of the businesses had similar methods of operation. Customers paid for access to terminals that offered games normally found in gambling casinos. If the players won a game instantaneously, they could accumulate credits, transfer credits, and redeem credits.

One of the defendants made unexplained large cash deposits into his account at a bank. The funds were purportedly proceeds from an internet business. The defendant had moved constantly among multiple states and large purchases were made at casinos, hotels, and airline companies.

The same defendant made deposits at other banks, including multiple cash deposits during the course of one day totaling over $10,000. A review of the account showed cash deposits made in uneven amounts and that the deposits were often conducted multiple times at multiple branch locations. The defendant transferred funds to a prepaid card company, and claimed to be self-employed with an internet business. The bank found no evidence of normal business activity.

Drug Trafficker Pleads Guilty to Structuring and Money Laundering Charges

A defendant was sentenced to Federal prison after he admitted to structuring dozens of bank deposits and withdrawals, in an attempt to conceal proceeds from marijuana and hallucinogenic mushroom sales. With detailed bank statements, prosecutors could prove structuring and money laundering in lieu of presenting evidence of drug trafficking.

The defendant and his accomplices grew high-potency marijuana and psilocybin mushrooms and shipped the drugs to customers throughout the country. Prosecutors documented numerous cash deposits that were made to his bank account at several branches in a distant state. Additionally, numerous cash withdrawals from the account were made from a local branch during a period of several months.

In the plea agreement the defendant admitted to having structured currency transactions to evade reporting obligations while violating other laws involving the distribution of marijuana and psilocybin mushrooms, as well as to having knowingly engaged in a monetary transaction involving criminally derived property from the distribution of marijuana and psilocybin mushrooms.

As part of a plea agreement with prosecutors, the defendant will be forced to forfeit a residence and other property.

Cocaine Dealer Sentenced to Life in Prison for Distribution, Structuring, and Money Laundering

BSA information played a key role in the investigation and prosecution of a major drug trafficker. The information allowed investigators and prosecutors to identify additional accounts as well as measures that the defendant took to hide his illicit gains.

A cocaine dealer was recently convicted and sentenced to life in prison. The defendant was convicted of conspiracy to distribute cocaine, conspiracy to structure financial transactions, structuring financial transactions, and several counts of money laundering. The defendant was ordered to forfeit property and funds, as the proceeds of his illicit activities.

The defendant was the leader of a drug organization that obtained cocaine from sources in states across the country and elsewhere. The defendant employed couriers to bring the drugs to his home, often using cars that he purchased with specially installed hiding places to conceal the drugs.

He titled a car and real property in the name of a nominee in order to hide assets. In addition, the defendant paid a nominee cash from drug proceeds, so that the nominee could pay personal expenses of the defendant. Finally, the defendant wired drug proceeds throughout the country using a phony name, and had co-conspirators make cash deposits of less than $10,000 in order to avoid bank reporting requirements and to hide the source of the cash.

A financial institution noted the high volume of credits to an account of the defendant and no identifiable employment information. Investigators were able to identify transactions made to conceal his illicit activities and cross reference it with his other accounts. The information also corroborated various aliases that the defendant used.

Conviction for Making False Statements

A federal judge sentenced the defendant to a prison term after a jury found the defendant guilty of several counts of making false statements to a federally insured bank.

The defendant owned a construction firm. A federally insured bank granted the defendant a working capital line of credit to be utilized for his construction business. The loan agreement specified that the defendant was permitted to borrow up to a specified percentage of the total amount of the firm's accounts receivable. As a condition of the agreement, he was required to file monthly accounts receivable reports. For each advance requested against the line of credit, the defendant was required to submit a borrower's certificate.

The reports and certificates submitted were false and overstated the total amount of accounts receivable. The defendant submitted records which falsely represented collateral with the intention to deceive the bank in order to draw more money from his line of credit. These false statements resulted in significant losses to the bank.

It was through a proactive review of BSA filings that the case came to the attention of law enforcement officials. As a result of the cooperation between law enforcement and the bank, the defendant was ordered to pay restitution.

Structuring and Tax Charges

A proactive review of BSA filings from several financial institutions led law enforcement to investigate the operator of a charitable organization who had structured over $1 million. The defendant pleaded guilty to structuring and the filing of a false tax return, and was sentenced to a prison term.

The defendant deposited substantial sums of currency into local bank branches by making over one hundred individual cash transactions in amounts of less than $10,000 to evade the reporting requirement, sometimes making deposits at multiple branches on the same day. Though he initially came under scrutiny for his structuring activities, authorities also found that he had filed a tax return that significantly understated his income. Additionally, the defendant claimed that he donated money to the charitable organization, but he later withdrew the money while still taking a charitable deduction on his taxes.

Illicit Wire Activity Destined for Sanctioned Country

Law enforcement initiated an investigation into a defendant for operating an unlicensed money transmitting business and assisting the business in the avoidance of Office of Foreign Asset Control (OFAC) sanctions on a designated country.

The defendant was convicted of violating the International Emergency Economic Powers Act (IEEPA), operating an unlicensed money transmitting business, and making false statements to a federal agency. A federal judge ordered the defendant to forfeit funds and sentenced the defendant to a multi-year prison term.

The defendant provided money transmitting services to residents of a sanctioned country by participating in the operation of a "hawala," a type of informal value transfer system in which money does not physically cross international borders through the banking system. The defendant used the hawala network to receive wire transfers from companies and individuals located in various countries, including some with a high risk for money laundering, into a personal bank account he maintained for this purpose in the United States.

An individual who resided outside the United States arranged the transfers into the defendant's account. The individual was associated with hawala operators in his country of residence. In addition, the individual attempted to move funds from a business and invest them in the United States. To accomplish this, the individual paid the hawala operators millions of dollars in foreign currency, and the hawala operators arranged to have corresponding amounts of U.S. dollars, which were already in

the United States or in bank accounts abroad, deposited into defendant's account. The owners of the dollars deposited into the defendant's account were dozens of companies and individuals in the U.S. and abroad who wanted to transfer funds to the country where the individual resided, a jurisdiction subject to OFAC sanctions.

The defendant facilitated these illegal transfers by accepting deposits into his personal bank accounts and then notifying the individual arranging the transfer or an out-of-country hawala operator, so that a corresponding amount of local currency could be disbursed. The hawala operators profited by manipulating the exchange rates to their benefit, and the defendant benefitted by using the millions of dollars he received into his account to purchase real estate and securities, and to pay hundreds of thousands of dollars toward personal expenses.

BSA information was instrumental in identifying the various accounts, wires, deposits, and patterns of activity.

Section 4 - Issues & Guidance

This section of *The SAR Activity Review* discusses current issues raised with regard to the preparation and filing of Suspicious Activity Reports (SARs) and provides guidance to filers. It reflects the collective positions of the government agencies that require organizations to file SARs. This issue highlights the value of Bank Secrecy Act (BSA) information and information sharing under 314(b).

Helping Your Board of Directors to Understand the Value of Bank Secrecy Act Information

By FinCEN's Office of Outreach Resources

In an effort to engage various financial institution types on Bank Secrecy Act (BSA) matters, FinCEN has been conducting outreach initiatives to financial institutions across the United States. The Financial Institution Outreach Initiative assists in FinCEN's ongoing work with the financial industry as financial institutions strive to comply with their responsibility to report certain financial information and suspicious activities to FinCEN, and assists in the fulfillment of FinCEN's responsibility to ensure this useful information is made available to law enforcement, as appropriate. The exchange of information, however, is not one-sided. Financial institutions provide FinCEN with feedback and sometimes request from FinCEN materials that may assist with BSA compliance.

FinCEN has received requests for materials that may assist BSA Officers with educating their Board of Directors on the importance, and use, of BSA data. This article is intended to serve as a resource for financial institutions as they work to inform Board members on the importance of maintaining a robust BSA compliance program. Compliance Officers may find the following information useful to highlight when presenting on BSA value to Boards of Directors.

* * * *

The work in which FinCEN and financial institutions collectively engage ensures an effective and successful fight against illicit activity, particularly as law enforcement confronts fraud and money laundering. FinCEN currently is in partnership with more than 300 law enforcement, intelligence, and regulatory agencies and remains committed to fighting money laundering and financial crimes. Additionally, more than 100 SAR Review Teams (multiagency task forces) operate across the country to review thousands of SARs each month. It is through these partnerships, using all the tools at its disposal and coordinating activities with its partners in both the public and private sectors, that FinCEN achieves its mission of enhancing U.S. national security, deterring and detecting criminal activity, and safeguarding financial systems.

Information financial institutions provide through the BSA and file with FinCEN can be the tip-off that starts an investigation. An officer's good instincts can, and do, result in the contribution of critical information that serves to set investigatory wheels in motion to track down suspected criminal activity. Examples of the cases that result from the use of BSA data for arrests and prosecutions can be found in this edition and previous editions of *The SAR Activity Review*, as well as on FinCEN's website.[28] These examples highlight how information received by financial institutions is combined with data collected by the law enforcement and the intelligence communities to connect dots in investigations and allow for a more complete identification of subjects, as well as banking patterns, travel patterns, and communication methods.

When an investigation is already underway, BSA information has added significant value by pointing to the identities of previously unknown subjects, exposing accounts and other hidden financial relationships, unveiling items of identifying information like common addresses or phone numbers that connect seemingly unrelated individuals, and, in some cases, even confirming locations of suspects at certain times. Law enforcement consistently affirms the value and reliability of BSA reports, which is a direct reflection of the diligence and training within financial institutions.

FinCEN uses technology to examine the entire BSA information base more broadly. When expertly queried, the data unmasks trend and patterns that hold signs of criminal or terrorist networks or emerging threats. Hidden in the wealth of

28. http://www.fincen.gov/law_enforcement/ss/

information, but easily revealed by skilled analysts with the right tools, are reliable and credible reports of mortgage fraud, check fraud, identity theft, and other suspected crimes. In other words, each financial institution provides FinCEN with a piece of a puzzle which, in the aggregate, provides a clear picture of illicit activities. One of the key reasons for FinCEN and law enforcement to proactively look for trends in BSA data that may assist prosecutions is because criminals are often creating new angles and opportunities to exploit the financial system. The United States Government is intensifying its efforts to help Americans against those, such as perpetrators of mortgage loan fraud, who seek to prey on the most vulnerable. Querying BSA data is a component to finding and combating these crimes.

With the booming housing market earlier this decade, mortgage loan fraud emerged as an issue, because there was a lot of money changing hands and it was easier to get a mortgage with minimal documentation. Now that the mortgage market has slowed, criminals are using loan modification and foreclosure rescue scams to prey upon innocent homeowners who are doing everything they can just to keep their homes. Through this effort, FinCEN and the Departments of Justice and Housing and Urban Development, the Federal Trade Commission and various state Attorneys General are working to combat fraudulent loan modification schemes and coordinate ongoing efforts across a range of Federal and State agencies to investigate fraud and assist with enforcement and prosecutions.

It is only through the contributions of financial institutions across the country that FinCEN is able to accomplish its mission of enhancing U.S. national security, deterring and detecting criminal activity, and safeguarding the financial system from abuse by promoting transparency in the U.S. and international financial systems. FinCEN's website provides information on BSA data support for complex investigations, strategic analysis, and how FinCEN fits into the global network of Financial Intelligence Units (FIUs). This information may be useful in reminding Board members that data submitted to FinCEN is not merely a requirement with which financial institutions need to comply to avoid regulatory repercussions, but a complex and integrated tool to combat a broad spectrum of crimes and help prevent terrorist acts.

Voluntary Information Sharing — Section 314(b) of the USA PATRIOT Act (31 CFR 103.110)

By FinCEN's Office of Outreach Resources

On September 26, 2002, regulations implementing section 314(b) of the USA PATRIOT Act became effective. These regulations are codified at 31 CFR 103.110. The regulations permit two or more financial institutions and associations of financial institutions[29] to share information with each other regarding individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities.[30] A financial institution or association of financial institutions that shares information pursuant to section 314(b) is protected from liability under the 314(b) safe harbor.[31] Participation in the section 314(b) information sharing program is voluntary and is utilized at the discretion of the participating financial institution. FinCEN, however, encourages financial institutions to participate in the 314(b) program in order to protect the integrity of the financial system and to mitigate institutional risk more effectively and efficiently.

In order to avail itself of the 314(b) safe harbor, a financial institution must, in part, notify FinCEN of its intent to share information under the 314(b) program,[32] and establish procedures to protect the security and confidentiality of 314(b) information. Also, prior to sharing information, a financial institution must verify that the other financial institution or association of financial institutions with which it intends to share information has provided the requisite notice to FinCEN. This

29. "Association of financial institutions" is defined at 31 CFR § 103.110(a)(3)

30. See 31 CFR § 103.110.

31. See 31 CFR § 103.110(b)(5). See, also *Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act*, FIN-2009-G002 (June 16, 2009).

32. Each financial institution or association of financial institutions that wishes to share information is required to provide notice to FinCEN by completing the registration form on the FinCEN website, https://www.fincen.gov/314b/314b_notification.php. The form may be completed and submitted electronically, or completed in paper format and mailed to the following address: FinCEN: P.O. Box 39, Mail Stop 100, Vienna VA 22183. The registration form should take only minutes to complete.

may be done by confirming that the other financial institution or association of financial institutions appears on the 314(b) list that FinCEN makes available to those financial institutions that have filed notice with FinCEN of their intent to share information through the 314(b) system. The financial institution may also confirm directly with the other financial institution or association of financial institutions that the requisite notice has been filed.

A financial institution participating in the 314(b) program is required to maintain adequate procedures to protect the security and confidentiality of information shared under the 314(b) program.[33] A financial institution participating in the 314(b) program is also required to designate a point of contact at the financial institution for sending and receiving 314(b) information sharing requests. FinCEN has been asked whether a financial institution's designated point of contact is the only individual permitted to send and receive information shared pursuant to the 314(b) program. The regulations implementing section 314(b) do not prohibit a financial institution from establishing policies and procedures that designate more than one person with the authority to participate in the financial institution's 314(b) program. In fact, a financial institution may find it useful to identify more than one appropriate individual to serve as the point of contact for those instances when the primary 314(b) contact is unavailable.

This issue's *Industry Forum* section discusses the topic of 314(b) information sharing through the lens of industry participants. Institutions may find the experiences of others to be informative as they work to develop and enhance their own 314(b) programs. Questions or comments regarding 314(b) information sharing should be addressed to the FinCEN Regulatory Helpline at 800-949-2732.

33. See 31 CFR § 103.110(b)(4).

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 present 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.

Section 314(b): To Share or Not to Share?

By: Jeffrey Halperin, Vice President, MetLife, representing MetLife on the Bank Secrecy Act Advisory Group

In an age of technological advances and large sums spent on anti-money laundering (AML) surveillance systems, the simple act of sharing information through direct communication between financial institutions remains a highly effective, yet often overlooked, tool in the fight against money laundering and terrorist financing activities.

Section 314(b) of the USA PATRIOT Act encourages financial institutions to share information that may be useful in detecting and preventing possible terrorist or money laundering activities by providing a "safe harbor" from liability for sharing such information. Many financial institutions, however, are reluctant to share information under Section 314(b) because of the complexity involved in determining which activities or transactions may be considered money laundering or, to a lesser extent, terrorist activity, or the fear that confidential information will somehow be inappropriately disclosed by a downstream recipient. Financial institutions should note, however, that as a condition for using the 314(b) process, all participating institutions must have policies to protect the confidentiality of the information shared.

On June 16, 2009, FinCEN sought to address these concerns and published interpretive guidance on the scope of permissible information sharing covered by Section 314(b). Under this guidance, FinCEN clarified Section 314(b)'s meaning of "money laundering" to include the "array of fraudulent and other criminal activities" known as specified unlawful activities ("SUAs") under 18 U.S.C. 1956 and 1957. Determining the appropriate SUA for a specific set of facts or circumstances, however, can be complex and may, if not clearly articulated, discourage participation.

Since participation in Section 314(b) information sharing as well as responding to a 314(b) request is voluntary, a firm's decision to share information is specifically its own. Experience shows that sharing information between financial institutions is a critical tool and should be used more often with less focus on form and more on substance. The way a firm approaches requesting information, however, can improve the timeliness and quality of the response. This article seeks to provide additional information from an industry perspective on SUAs that relate to fraudulent and other criminal activities, as well as provide useful tips on how to frame and follow-up on 314(b) requests to ensure that requests are reviewed in a timely manner and responses include useful information.

Background

Any financial institution, as defined in 31 CFR 103.110(a)(2), may participate in information sharing under Section 314(b). Participation is voluntary and a financial institution may choose, at any point, not to share information with another firm. Section 314(b) encourages information sharing because Congress understood that each financial institution often has only a "snapshot" of a particular customer or financial transaction. By sharing information about the transaction, two unrelated financial institutions can provide clarity around whether a transaction is suspicious or merely atypical. To underscore this and encourage sharing, Congress provided a "safe harbor" from liability for such sharing. Section 314(b)'s "safe harbor" is, however, limited to information exchanges related to "activities that the financial institution or association suspects may involve possible terrorist activity or money laundering."

Under Section 314(b), information may only be shared between participating institutions that have filed a Notice of Intent to Share and designated an individual point of contact. The Notice can be submitted electronically on FinCEN's website or a hard copy can be mailed to FinCEN. The notice is simple to complete and is effective for one year from the filing date. Continued participation requires an annual re-filing. FinCEN provides written confirmation shortly after its receipt of notice. Given the potential liabilities associated with not being able to rely on the safe harbor, financial institutions should maintain copies of FinCEN's confirmation letters as evidence that notice was received and is in effect.

Before sharing information, firms must verify that the corresponding financial institutions are also participants in the program. To that end, FinCEN periodically distributes to participating firms a password-protected list of Section 314(b) participants and their designated contacts, including phone numbers and e-mail addresses for the designated contacts. Firms sharing information may then verify their counterparties' participation by checking the 314(b) list. Firms can also verify participation directly with other financial institutions.

It is important to note that if a financial institution has not notified FinCEN of its intent to share information under 314(b), then it is not eligible to participate in the program and will not benefit from the protections of the safe harbor. As such, other firms may be reluctant to contact that entity, even with clear indication of illicit activity going through that financial institution. In this circumstance, industry participants may risk missing opportunities to share valuable information that may be relevant to their AML programs.

Section 314(b) requires financial institutions that participate in information sharing to maintain appropriate procedures to ensure that information shared is kept confidential. In addition, information received can only be used for the purposes of identifying and reporting on money laundering or terrorist activities; determining whether to establish or maintain an account or to engage in a transaction; or assisting the receiving firm in complying with any requirements under the rule. Although the rule does not require that 314(b) requests be in writing, it is a best practice to initiate requests in writing to the designated contact(s).

Covered Information

As described above, activities that involve "money laundering" are within the scope of information that may be shared. FinCEN's recent guidance makes clear that "money laundering" includes those activities defined as SUAs under 18 U.S.C. 1956 and 1957. Many of the SUAs describe offenses that do not often impact financial institutions, such as crimes against foreign nations, international airports, or Federal officials. That said, section 1956(c)(7)(D) and section 1961(1)(A)-(G), for example, define SUAs that relate to a number of types of fraud, including those related to banking and transactions, loan and credit applications, Federal Deposit Insurance transactions, bank entries, loan or credit applications, and federal credit institution entries. It is important, though, that financial institutions understand that the number of criminal activities covered within the scope of "money laundering" is quite broad.

Tips on Sharing

Once a firm has identified activity that relates to an appropriate SUA, a well constructed request for information under Section 314(b) improves firms' responses in terms of both timeliness and usefulness. Under the regulation, a request is permitted to be written or verbal. Sometimes a verbal request may be better due to the rapid nature of an investigation. The important point is to be clear as to the basis for the request and be specific about what you are requesting. Following up a verbal request with an email is always an effective way to provide a reminder and to "paper the file."

Directing 314(b) requests to the appropriate individual helps to speed the process along. Although requests sent to the point of contact listed in FinCEN's 314(b) list are often forwarded internally for response, it is helpful to address requests directly to the attention of the contact. It is also helpful to call the designated 314(b) contact to make sure that the request has been received, that the point of contact has not changed or to determine whether there is another individual at the institution who can better handle the request. In addition, if an individual other than the designated point of contact is initiating a request, it is good practice to copy the point of contact on the request and to provide details about the sender's relationship to the contact person.

The content of the 314(b) request should also be carefully crafted to ensure a valuable response. It should clearly establish a basis in the rule's requirements by specifically requesting information sharing pursuant to 314(b) and describing how the activity relates to possible money laundering or terrorist activity. In addition, requests related to money laundering should include details of the applicable SUAs. When sending a written request or following up a verbal request in writing, one should indicate the basis for the request and provide as many details as possible as to how it relates to an SUA.

The request should then include specific details of the activity or transaction for which information is sought. At this point, the sender is actually sharing information, so it is important to have first confirmed the recipient's participation in the 314(b) program and to have documented that step internally. The description should include the date or date range of the activity or transaction, the amount involved, the account number(s) at both institutions, the account title or designation, the branch or location involved, and any other information that may facilitate the recipient's research.

Clearly articulated requests are more likely to result in useful responses. Although this is often overlooked, all requests should describe, with as much specificity as possible, the type of information that is being requested. If, for example, the request relates to the source of funds at the other financial institution, it should indicate specifically what information about the source of funds would be useful to the requesting firm. Likewise, if the request relates to transactional activity between the two firms, describe the transactions in detail, and request specific information necessary to support the investigation. Such a request may even cause the receiving firm to start its own investigation. It is also important to note that the non-bank financial institution may have a very limited view of the customer or the transaction, so its request may appear broad due the limited information. Remember that the request will be made to another "AML professional," so it is worthwhile to request their opinion on whether there are other indicators within their data that cause them concern from a money laundering or terrorist financing perspective.

Appropriate follow-up also can help ensure timely responses. A first step toward shortening response time is to communicate to the recipient when its response is requested and why timeliness is important. In addition, recipients of 314(b) requests are often engaged in their own investigations and may not appreciate how the information may be useful to their firm. So, providing specific details about the matter, as described above, is important. It is not unusual for firms to take over two weeks to respond to requests, so follow-up within a reasonable time from the date of the initial request is appropriate. When determining a reasonable time for follow-up, consider the scope and level of detail of the information requested. As a final measure, a telephone call to the 314(b) point of contact can often trigger a response. Establishing a relationship with the point of contact at a firm can also help facilitate this process and build credibility to the extent that the receiving firm understands that the request complies with the rules and prior exchanges of information have been valuable. It can also be helpful to focus the request by answering any questions that the recipient might have.

Benefits of Sharing

A meaningful exchange of information between financial institutions is a powerful tool for detecting and preventing money laundering. If properly utilized, Section 314(b) allows firms to significantly expand the range of information available for assessing potentially suspicious activity or accounts without increasing risk. The information received by a requesting firm may provide the firm with details it may not have had, for example, about the source of a customer's funds. The information received by a requesting firm can also help a firm's decision to close an account or decline to open a new account. At the same time, a financial institution may proactively use 314(b) to alert other firms of information about their client that they might not have been aware of before the information sharing. The ultimate result for information sharing under 314(b) is to confirm or deny a requesting firm's suspicions that potential money laundering could be occurring through their firm.

Law enforcement agencies also can benefit under 314(b) when the sharing of information between two institutions results in the filing of a Suspicious Activity Report (SAR). In some cases, the information provided may be enough to trigger the decision to file a SAR, and SARs that include information derived from more than one financial institution are likely to benefit law enforcement agencies by providing a more detailed and complete account of the transactions reported. Ultimately, the information provided by the filing institution may prompt law enforcement to open an investigation or add to an existing investigation.

Closing

Used properly, Section 314(b) expands the depth and scope of information available to firms in their effort to mitigate the risks posed by potential money launderers. In addition, firms that share information under Section 314(b) reduce their exposure to fraud and other costly financial crimes. Most important, as noted by Director Freis on a number of occasions, the act of sharing information between financial institutions is essential to combating financial crime and ultimately increasing the integrity of the financial system.

Section 6 - Feedback Form

Financial Crimes Enforcement Network

U.S. Department of the Treasury

Tell Us What You Think

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. The form can be faxed to FinCEN at (202) 354-6411 or accessed and completed online at http://www.fincen.gov/feedback/fb.sar.artti.php. Questions regarding The SAR Activity Review can be submitted to sar.review@fincen.gov. For all other questions, please contact our Regulatory Helpline at 1-800-949-2732.*
Please do not submit questions regarding suspicious activity reports to the SAR Activity Review mailbox.

A. Please identify your type of financial institution.

Depository Institution:
__ Bank or Bank Holding Company
__ Savings Association
__ Credit Union
__ 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**
__ **Dealers in Precious Metals, Precious Stones, or Jewels**
__ **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 - Issues & Guidance	1	2	3	4	5
Section 5 - Industry Forum	1	2	3	4	5
Section 6 - 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. 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.

_____
_____
_____
_____

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

_____
_____
_____
_____

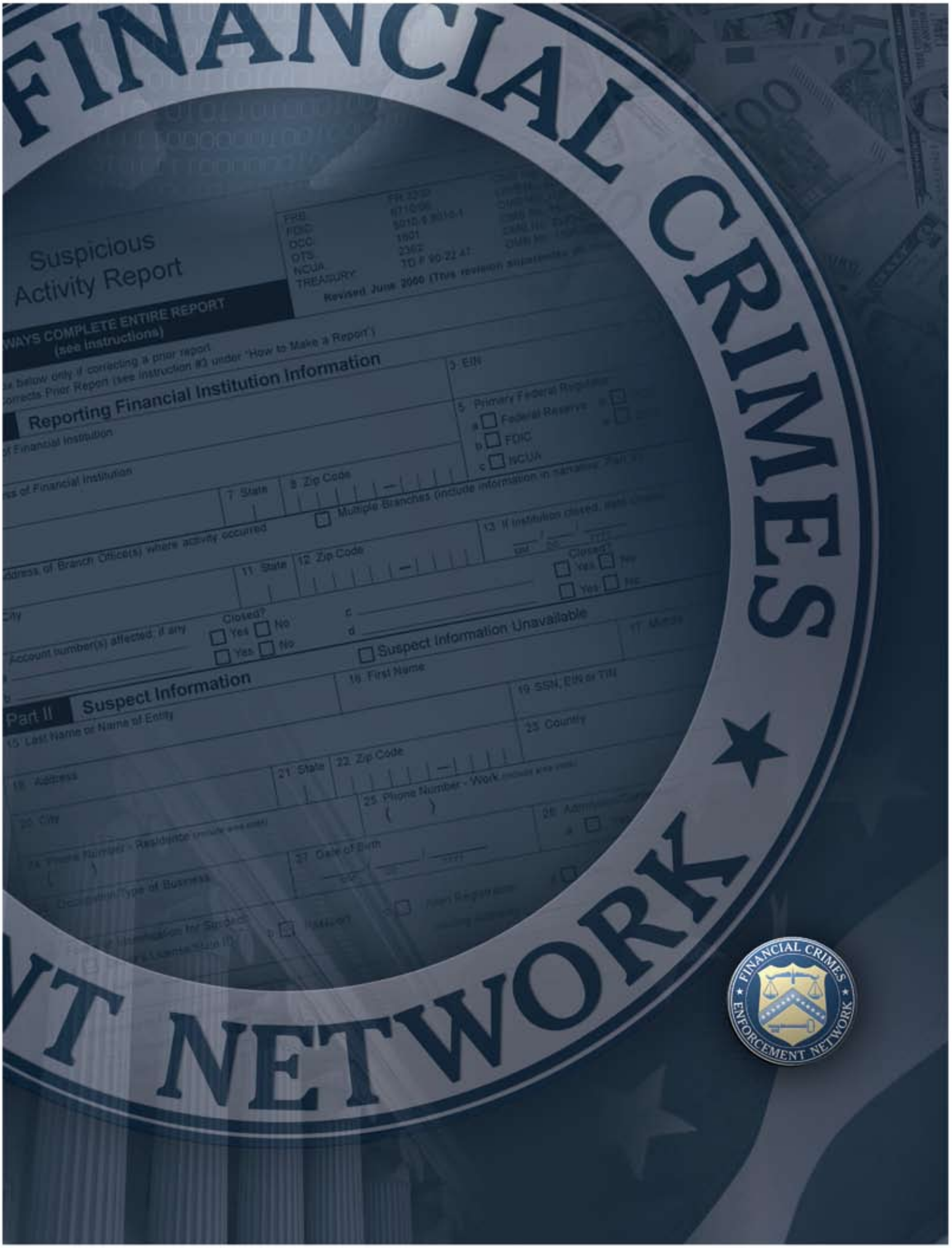
G. Which of the previous issues have you read? (Check all that apply)

[ ] All Issues

[ ] Issue 1 - October 2000
[ ] Issue 2 - June 2001
[ ] Issue 3 - October 2001
[ ] Issue 4 - August 2002
[ ] Issue 5 - February 2003
[ ] Issue 6 - November 2003
[ ] Issue 7 - August 2004
[ ] Issue 8 - April 2005
[ ] Issue 9 - October 2005
[ ] Issue 10 - May 2006
[ ] Issue 11 - May 2007
[ ] Issue 11 - October 2007
[ ] Issue 13 - May 2008
[ ] Issue 14 - October 2008
[ ] Issue 15 - May 2009
[ ] Issue 16 - October 2009
[ ] Issue 17 - May 2010

The *SAR Activity Review* **Index** is available on the FinCEN website at:
http://www.fincen.gov/news_room/rp/files/reg_sar_index.html.
For your convenience, topics are indexed alphabetically by subject matter.

The **Archive of Law Enforcement Cases** published in *The SAR Activity Review* can be accessed through the following link:
http://www.fincen.gov/news_room/rp/sar_case_example.html.


FINANCIAL CRIMES
NETWORK
Suspicious
Activity Report
Reporting Financial Institution Information
Suspect Information
Part II
FINANCIAL CRIMES
ENFORCEMENT NETWORK