The SAR Activity Review

Trends Tips & Issues

Issue 15

In focus: The Securities and Futures Industries

Published under the auspices of the BSA Advisory Group.
May 2009

Financial Crimes Enforcement Network

The SAR Activity Review

Trends Tips & Issues

Issue 15

In focus: The Securities and Futures Industries

Published under the auspices of the BSA Advisory Group.
May 2009

Table of Contents

The SAR Activity Review **Index** is now 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[1] to provide meaningful information about the preparation, use, and value of Suspicious Activity Reports (SARs) and other Bank Secrecy Act reports filed by financial institutions.

This edition focuses on the securities and futures industry and addresses several noteworthy topics. Articles in the *Trends & Analysis* section include an assessment of SARs filed by the securities and futures industry by FinCEN's Office of Regulatory Analysis as well as information from staff of the Securities and Exchange Commission (SEC) on how to file SARs, the SEC's use of SARs and the consequences to regulated institutions for failure to file. An article by staff from the SEC and FINRA (Financial Industry Regulatory Authority) looks at how securities regulators review SARs during examinations.

As always, the law enforcement cases in Section 3 demonstrate how important and valuable BSA data is to the law enforcement community. Cases in this section cover the securities industry, Ponzi schemes and mortgage fraud cases. In the *Issues & Guidance* section, we provide guidance on identifying and reporting suspicious transactions for introducing and clearing brokerage firms and SAR form completion when reporting identity theft. FinCEN's Office of Enforcement also discusses why covered financial institutions should consider seeking global resolution to potential enforcement actions. In the *Industry Forum* section, we get an industry viewpoint on how broker-dealers can ensure effective SAR programs.

---

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; 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.

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.

Feedback from FinCEN

Readers of *The SAR Activity Review* frequently inquire through their feedback to us about the frequency and focus of the publication. Specifically, readers want to know how often it is published, whether it can be published more frequently (such as quarterly, or even once a month for "hot topics"), and whether issues can be published specific to a geographic region or industry.

Beginning with Issue 11, published in May 2007, FinCEN moved to a semi-annual publication schedule for the *Trends, Tips & Issues* publication. It is now published in May and October each year. Because of limited resources, we are unable to publish a SAR Activity Review specific to each industry or to a geographic region or more frequently than the current schedule.

In 2008, FinCEN began including information regarding Currency Transaction Report (CTR) filings in *The SAR Activity Review*. Another change we have made, beginning with a securities industry theme as the focus for much of this issue, is to alternate between a theme-based issue for the May publication and our standard general issue for the October publication. With each May issue, we will explore a different industry or issue in more depth and we encourage readers to consider how the information presented can be applied to their own industry.

FinCEN relies on the valuable contributions of people from the financial industry and our regulatory and law enforcement partners, as well as FinCEN staff, to develop the articles for each issue. Many of the contributors to the publication also lend their support and expertise to a number of our other publications, such as *The SAR Activity Review – By the Numbers*, the companion piece to *Trends, Tips & Issues*, as well as our numerous analytical products, such as the Insurance SAR study and the Mortgage Loan Fraud studies.

You can subscribe to FinCEN Updates under "What's New" on the FinCEN website, www.fincen.gov, to receive notification of when *The SAR Activity Review* is published. As always, your comments and feedback are important to us. We have included a feedback form in Section 6; please take a moment to let us know if the topics chosen for this issue are helpful.

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

Lilly Thomas
Regulatory Counsel
Independent Community Bankers of America
1615 L Street, NW, Suite 900
Washington, DC 20036-5623
Phone: 202-821-4409
lilly.thomas@icba.org
www.icba.org

Barbara Bishop
Regulatory Outreach Project Officer
Financial Crimes Enforcement Network (FinCEN)
PO Box 39
Vienna, VA 22183
Phone: 202-354-6400
sar.review@fincen.gov

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

Section 1 — Director's Forum

Welcome to the fifteenth edition of *The SAR Activity Review - Trends, Tips & Issues*, FinCEN's semi-annual publication designed to continue the dialogue among those of us in the law enforcement, financial, and regulatory fields who share common interests in the value of Suspicious Activity Reports (SARs) and the wealth of vital information they contain. This dialogue among SAR users and providers has rarely, if ever, been as important as it is today. America's financial system is undergoing unusual and persistent strains that not only create opportunities for fraud and abuse but also challenge compliance professionals and law enforcement officials to remain vigilant under stressful circumstances and limited resources.

It is becoming more apparent that the current urgent conditions we together face have melted away many debates of the past and have strengthened the partnership and spirit of cooperation between our community of users and providers of SARs. Few now question the tremendous value that SARs present to law enforcement, and recent reports from the Government Accountability Office (GAO) as well as FinCEN's strategic mortgage fraud reports have provided ample and compelling evidence of the importance of SARs. Last month, the Obama Administration launched a major initiative to target mortgage loan modification and foreclosure rescue scams and coordinate anti-fraud activities across federal and state government lines and with the private sector. As key players, Treasury and FinCEN announced an advanced targeting effort, centered around the collection and synthesis of a wide range of information, including SARs and other BSA data, about bad actors in the loan modification industry, to combat these schemes. A critical part of this effort depends on financial institutions and in order to help institutions provide more useful information to law enforcement, FinCEN has issued an advisory alerting financial institutions to the risks of emerging schemes. It identifies certain "red flags" that may indicate a scam and requests that financial institutions include the phrase "foreclosure rescue scam" in the narrative sections of all relevant SARs. Our community should be very proud of this recognition of the power and utility of SARs.

Every industry with SAR filing responsibilities is an equally important member of the team. Law enforcement investigators depend on the experience and instincts of compliance professionals to form the frontline against fraud. As recent market occurrences have shown, no industry is immune from the damage that fraud and money laundering can bring and, as illustrated by FinCEN's recent report, *Mortgage Loan Fraud Connections with Other Financial Crime*, criminals are not containing their activities to any single industry, or for that matter, country.

This issue of *The Review* emphasizes the role and responsibilities of the Securities and Futures Industries. Though relatively new to SAR filing responsibilities – brokers and dealers in securities have been required to report suspicious transactions since 2003; futures commission merchants and introducing brokers in commodities since 2004; and mutual funds since 2006 – the information that law enforcement gains from this sector is increasingly valuable. For example, the Commodities and Futures Trading Commission (CFTC) has recently credited FinCEN and SAR data with a number of important enforcement actions concerning Ponzi schemes and fraud.

Inside this *Review*, the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) have provided articles that offer in-depth looks at their use of SAR data. Also, the *Industry Forum* offers advice from experts on the challenges of spotting unusual market activity when recent market activity has been historically unusual.

As usual, you will also find outlines of many more law enforcement cases which describe the successful use of SARs and Currency Transaction Reports (CTRs) to combat crime. Again, I sincerely look forward to your feedback and comments.

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

Section 2 - Trends & Analysis

This section of *The SAR Activity Review* focuses on suspicious activity reporting by the securities and futures industry. An article by FinCEN's Office of Regulatory Analysis highlights findings of an assessment of SAR-SF filings. An article by SEC staff provides guidance on how to file SARs and discusses how SARs are used and the consequences to a financial institution when they fail to file SARs. Finally, staff from the SEC and FINRA provide feedback on some of the questions raised during the examination process.

An Assessment of Suspicious Activity Reports Filed by the Securities and Futures Industry

By FinCEN Office of Regulatory Analysis

Brokers and dealers in securities have been required to file suspicious activity reports since January 1, 2003.[2] In May 2004, the regulatory definition of "financial institution" was expanded to include futures commission merchants and introducing brokers in commodities, requiring that they also comply with the recordkeeping and reporting requirements of the Bank Secrecy Act (BSA). In this article, we highlight key findings from an assessment of Suspicious Activity Reports filed by the Securities and Futures Industries (SAR-SF) between January 1, 2003 and December 31, 2008, for money laundering, terrorist financing and other financial crimes.[3]

2. See 31 CFR § 103.19 and 67 F.R. 44048 (July 1, 2002).

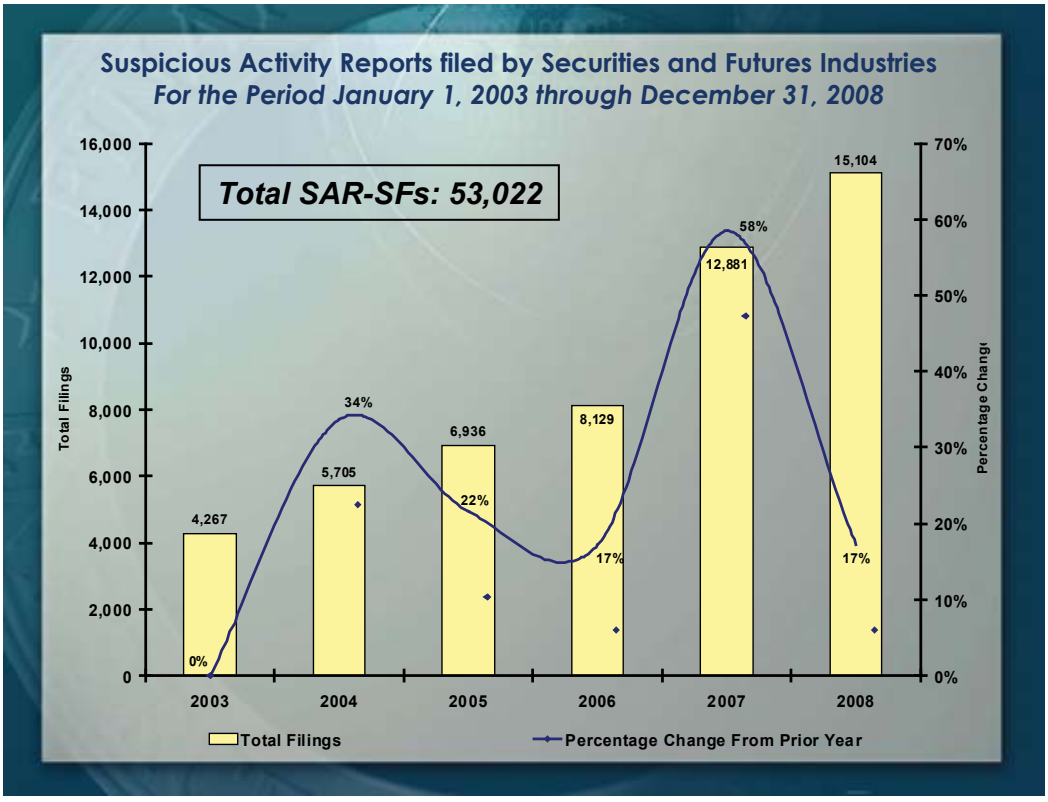
3. Please note: Futures commission merchants and introducing brokers in commodities were not required to report suspicious activity until May 2004, although the analysis for this study dates back to January 1, 2003. Insurance companies do not have a dedicated SAR form, and so they have been instructed to use the SAR-SF. Insurance companies filing SAR-SFs are included in the totals; however, analysts eliminated these from the study group. For information regarding suspicious activity reporting by certain insurance companies, see FinCEN's *Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings April 2008* at http://www.fincen.gov/news_room/rp/reports/pdf/Insurance_Industry_SAR.pdf.

FinCEN analysts examined SAR-SFs to identify trends and patterns relating to filing volume, type of reporting institution, characterization of suspected activities, and filings by instrument type. We also include summaries from a sample of SAR-SF narratives reviewed to identify typologies and potential emerging threats to this industry. FinCEN continues to examine SAR-SFs and plans to release a more detailed assessment later in 2009.

Filing Trends

In 2003, the first year suspicious activity reporting was required for securities brokers and dealers, the securities industries filed 4,267 SARs. The annual volume of SAR-SF filings has increased every year since then, with 15,104 reports received by FinCEN in 2008. In the six year period since suspicious activity reporting requirements were extended to the securities and futures industries, covered institutions have filed a total of 53,022 SAR-SFs.[4] Graph 1 depicts the annual filing volume and the percentage change in reporting from year to year.

Graph 1



4. See *By the Numbers*, FinCEN's bi-annual companion publication to *The SAR Activity Review-Trends, Tips & Issues*, for more numerical information at http://www.fincen.gov/news_room/rp/sar_by_number.html.

Types of Reported Suspicious Activity

Between January 1, 2003 and December 31, 2008, filers marked the "Other" field (Field 30t) on the SAR-SF form as the most prevalent characterization of suspicious activity, followed by Money Laundering/Structuring (Field 30l). Exhibit 1 identifies the top five characterizations of suspicious activity reported for the review period. These five characterizations together comprise 61 percent of all suspicious activity reported in SAR-SFs filed since 2003.

Exhibit 1: *Top Five Characterizations of Suspicious Activity**

Type of Suspicious Activity	Filings	Percentage
Other	17,998	20.74%
Money Laundering/Structuring	14,637	16.87%
Identity Theft	7,512	8.66%
Significant Wire or Other Transactions Without Economic Purpose	6,700	7.72%
Check Fraud	6,125	7.06%

*Some SAR-SFs may list multiple suspicious activities.

Exhibit 2 depicts the percentage change observed in 2008 SAR filings compared to the previous year for all categories of suspicious activity listed in Part II, Field 30. Reported activities that showed an increase from 2007 to 2008 are highlighted.

Exhibit 2: Suspicious Activity Comparison*: CY 2007 to CY 2008

Type of Suspicious Activity	2007	2008	Percentage Change
Bribery/Gratuity	52	44	-15%
Check Fraud	1,232	1,197	-3%
Computer Intrusion	1,241	967	-22%
Credit/Debit Card Fraud	410	800	95%
Embezzlement/Theft	592	851	44%
Forgery	392	492	26%
Futures Fraud	20	27	35%
Identity Theft	2,089	1,947	-7%
Insider Trading	388	499	29%
Mail Fraud	326	523	60%
Market Manipulation	1,470	1,460	-1%
Money Laundering/Structuring	3,994	4,037	1%
Other	3,938	5,288	34%
Prearranged or Other Non-Competitive Trading	145	143	-1%
Securities Fraud	1,520	1,856	22%
Significant Wire or Other Transactions Without Economic Purpose	1,413	1,813	28%
Suspicious Documents or ID Presented	808	802	-1%
Terrorist Financing	50	32	-36%
Unknown/Blank	145	122	-16%
Wash or Other Fictitious Trading	194	181	-7%
Wire Fraud	1,615	1,831	13%

*Some SAR-SFs may list multiple suspicious activities.

Filing Institutions

SAR filings from the securities and futures industries were received from a variety of filing institutions. While many of the institutional categories identified in Field 51 (Type of Institution or Individual) on the SAR-SF form are not mutually exclusive, the majority of the institutions self-identified as either clearing securities brokers

or introducing securities brokers. Furthermore, collectively, the clearing securities brokers, introducing securities brokers, and securities dealers filed the majority of the SAR-SFs during the entire period of the study. Six types of reporting institutions filed more than 1,000 SAR-SFs in 2008. Exhibit 3 lists those types of institutions.

***Exhibit 3:** Top Six Reporting Institutions in 2008**

Type of Institution	Number of SARS Filed
Securities Brokers-Clearing	5,391
Securities Brokers-Introducing	4,626
Securities Dealer	3,469
Investment Company–Mutual Fund	1,874
Affiliate of Bank Holding Company	1,853
Investment Advisor[5]	1,430

*Some SAR-SFs may list multiple reporting institutions.

Instrument Type Reported

"Cash or equivalent" (Field 23b) remains the most commonly reported instrument type used in transactions or activities that have been identified by filers as suspicious. The top five corresponding characterizations of suspicious activity reported where "cash or equivalent" was the instrument type were check fraud, identity theft, money laundering/structuring, significant wire or other transactions without economic purpose, and wire fraud. Furthermore, SAR-SF filers listed "stocks" as the second most reported instrument type. Computer intrusion, identity theft, market manipulation, securities fraud, and wire fraud ranked as the top five characterizations of suspicious activity associated with stocks.

5. This statistic reflects Investment Advisors who identified themselves as such on the SAR-SF (box 51j). Investment advisors are not currently subject to AML requirements and SAR filing requirements but may voluntarily file a SAR.

Suspicious Activity Identified in SAR-SF Narratives

The following list of the most frequently cited alleged suspicious activities includes examples of specific activities included in the SAR narratives.

Structured Deposits and Withdrawals:

- Structured check withdrawals from funds that originated from a margin loan against the assets held in the customer's account. No trade had occurred in the account since it had been opened.
- Deposits of multiple postal money orders and cashiers checks in amounts under the BSA reporting requirements. When asked about the deposits, the customer stated the purchasers who bought his home gave him postal money orders and cashier checks as part of the payment.
- Structured cashiers check purchases, check or money order deposits, cash withdrawals and wire transfer activity done to avoid the Currency Transaction Report (CTR) filing requirements. On occasion, individuals purchased money orders or cashiers checks at the same location but with different tellers and, at other times, at different locations. Destinations for some wire transfers included Africa, Australia, Brazil, China, New Zealand, Singapore, Switzerland and Taiwan.
- Structured deposits from an electronic payment and money transfer business, which did not correspond to the purchase of any merchandise.

Identity Theft:

- Individuals with trade accounts who became victims of identity theft.

Possible Terrorist Financing:

- Customers purportedly having business relationships with individuals and charitable organizations suspected of financing terrorist organizations.
- Login history of customer trade accounts from Internet protocol addresses routed through Canada, France, Iran, Jordan, Nigeria, United Arab Emirates, and United Kingdom. Filing institutions expressed concern that the account holders supposedly violated sanctions by accessing U.S. financial institutions online while in Iran. Furthermore, SAR narratives stated that deposit and withdrawal activity and unusual address connections might have indicated money laundering and/or terrorist financing.

- Client's withdrawals structured to possibly avoid the CTR reporting requirements. Further review by the filer of the source of funds revealed a dissident of an African country who is currently residing in Europe. According to the SAR-SF narrative, officers of the securities firm suspected the account holder's business, supposedly a shell company, was designed to facilitate the laundering of illicit funds. The filer further stated that potential ties to this particular African country presented concern that the funds involved possibly were used for terrorist financing.

Suspected Money Laundering or Tax Evasion:

- Trading account indicating an attempt to launder funds through stock transfers.
- Brokerage account receiving an excessive number of money order deposits which, according to the filer, resembled money laundering/structuring.
- Multiple postal money order deposits in amounts that appeared structured, possibly to avoid currency reporting requirements. The deposits did not support trading activity, and may have indicated an attempt to launder funds or evade taxes.
- Multiple customers with trade accounts internally transferring assets and funds. The utilization of the same address was the common thread between the parties. The filer stated that the activity might have indicated money laundering or terrorist financing.

Suspicious Wire Transfers:

- An unusual and unexplainable pattern of activity involving deposits from an electronic payment and money transfer business and incoming wire transfers followed by ATM withdrawals or wire transfers to foreign locations.
- An account with debit card purchases and cash advance transactions in South and Central America and the United States. Also, wire transfers from New York and from Miami, Florida disbursed at locations throughout one South American country known for its drug cartels and for having connections to a terrorist organization.
- A trading firm detected a pattern of funds flowing through a customer's account where wire transfers were deposited into the customer's account from a bank. The customer then used the funds to write checks or make wire transfer withdrawals paid to the order of a casa de cambio located in Mexico.

Other Notable Suspicious Activity:

- Amounts deposited into trading accounts that exceeded the customer's annual income and net worth.
- An individual submitting three account applications online to a registered broker-dealer firm. A check for approximately $150,000 was deposited into one of the accounts. When attempting to verify the check, the filer learned that it was counterfeit and immediately closed the account. Further investigation by the firm revealed that the individual used a false social security number, date of birth, name and address.
- A customer identifying himself as a tax attorney was concerned with commission amounts and looking for "no-load" mutual funds. It appeared that the activity in the account did not correspond with the selected time horizon of 10+ years. Also, the filer's search of an attorneys' database did not reveal any name matches for the customer despite his claims to being a tax attorney.

Conclusion

SAR-SF narratives analysis revealed much of the reported suspicious activity to be structuring of deposits or withdrawals using cash or equivalent to evade CTR filing requirements, which filers believed may have represented possible tax evasion, money laundering, terrorist financing or other financial crimes. Several SAR-SF narratives noted clients attempting to utilize their trading accounts for purposes other than investments or conducting unusual and unexplainable patterns of deposits followed by withdrawals or wire transfers to international locations. Multiple SAR-SF narratives reported alleged terrorist financing through charitable organizations. The filers noted some clients engaged in business relationships with individuals and organizations allegedly financing terrorist organizations. Later this year, FinCEN plans to publish a full report describing the findings from its assessment of SAR-SFs filed since 2003.

Suspicious Activity Reports in the Securities Industry: How to File a SAR, How SARs are Used, and the Consequences for Failure to File

By Staff of the Securities and Exchange Commission[6]

One of the cornerstones of the Bank Secrecy Act (BSA)[7] is the requirement that financial institutions monitor for, and report to the Financial Crimes Enforcement Network (FinCEN), suspicious activity. This reporting is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes.

Following the USA PATRIOT Act's[8] amendments to the BSA, broker-dealers and mutual funds (in 2003 and 2006, respectively) became subject to regulations requiring them to file Suspicious Activity Reports (SARs) with FinCEN on Form 101, generally referred to as the SAR-SF form.[9] The BSA, SEC and self-regulatory organization rules and regulations collectively require firms to establish and implement procedures that can reasonably be expected to detect and cause the reporting of suspicious transactions.

---

6. This article was prepared by staff in the Securities and Exchange Commission's (SEC or Commission) Division of Trading and Markets, with assistance from the staff in the Commission's Division of Enforcement (Enforcement) and Office of Compliance Inspections and Examinations (OCIE), but does not necessarily represent any staff views. The Securities and Exchange Commission, as a matter of policy, disclaims responsibility for any private publication or statement by any of its employees. The views expressed in this document do not necessarily represent the views of the Commission, or the members of the staff of the Commission.
7. The Currency and Foreign Transactions Reporting Act of 1970 (commonly referred to as the Bank Secrecy Act) is codified at 31 U.S.C. 5311, *et seq*. The regulations implementing the Bank Secrecy Act are located at 31 CFR Part 103.
8. Pub. L. No. 107-56, 115 Stat. 272 (2001).
9. See 31 CFR 103.19 and 103.15. The SAR-SF form is available at http://fincen.gov/forms/bsa_forms/.

Factors to Consider When Filing SARs

Mechanics of Filing

A SAR can either be mailed to a processing center or filed electronically on a secure website accessible on the Internet using the BSA E-Filing system.[10] In addition to supporting electronic filing of individual or batch BSA forms, such as SAR-SF forms, the system also allows filers to exchange secure messages with FinCEN. FinCEN also uses the system to issue advisories and system updates to the user community. FinCEN promotes the use of BSA E-Filing because it is more efficient, faster, and more secure than paper filing.

Process for Filing

The SAR must be filed no later than 30 calendar days from the date of the initial detection of the suspicious activity. If no suspect can be identified, the time period for filing a SAR is extended to 60 days. FinCEN has provided guidance that "initial detection" does not mean the moment a transaction is highlighted for review.[11] The time to file a SAR starts when a firm, in the course of its review or on account of other factors, is able to make the determination that it knows, or has reason to suspect, that the activity or transactions under review meet one or more of the definitions of suspicious activity. Specifically, the 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulations. Of course, a review must be initiated promptly and completed in a reasonable period of time.[12] Firms should maintain some type of record reflecting the date the transaction was

10. Additional enrollment information about FinCEN's BSA Direct E-Filing system is available at http://bsaefiling.fincen.treas.gov.
11. The SAR Activity Review, Trends Tips & Issues, Issue 10, at 44-46 (May 2006). See http://www.fincen.gov/sarreviewissue10.pdf.
12. An expeditious review is recommended and can be of significant assistance to law enforcement.

deemed suspicious. In situations involving violations of law requiring immediate attention, the firm should immediately notify appropriate law enforcement and supervisory authorities,[13] in addition to filing a SAR.

Firms also should remain cognizant of the need to comply with suspicious activity reporting obligations even where other BSA obligations, such as customer identification requirements, may not apply. For example, every clearing firm's anti-money laundering program should contain risk-based policies, procedures, and controls for assessing the money laundering risk posed by its clearing arrangements, for monitoring and mitigating that risk, and for detecting and reporting suspicious activity.[14]

Unless jointly filing a SAR, each broker-dealer involved in a transaction must individually identify and report suspicious activity. Only one SAR is required to be filed by a firm so long as the SAR includes all the relevant facts concerning the transaction and the names of all entities. In the case of a jointly filed SAR, each entity should keep a copy of the SAR. In addition, in adopting the SAR rule, FinCEN acknowledged that the rule does not require a firm to alter its relationship with its customers in a way that is inconsistent with industry practice.[15] FinCEN noted, for example, that based on the nature of the services that a broker-dealer provides to their customers, certain types of broker-dealers will have more information available to them in making suspicious activity determinations than other types of broker-dealers.[16]

---

13. See, e.g., AML Source Tool for Broker-Dealers, Part 14: Useful Contact Information, available at http://www.sec.gov/about/offices/ocie/amlsourcetool.htm. As provided in the SAR rules, in situations involving violations that require immediate attention, firms must immediately telephone an appropriate law enforcement authority in addition to filing a SAR. Additionally, firms wishing to voluntarily report suspicious transactions that may relate to terrorist activity can call the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) hotline at 1-866-556-3974. Broker-dealers may also, but are not required to, contact the SEC to report situations that may require immediate attention by the SEC. The SEC SAR Alert Message Line number (202-551-SARS (7277)) should only be used in cases where a broker-dealer has filed a SAR that may require immediate attention by the SEC and wants to alert the SEC to the filing. Calling the SEC SAR Alert Message Line or FinCEN's hotline does not alleviate the broker-dealer's obligation to file a SAR or notify an appropriate law enforcement authority.
14. See Customer Identification Program Rule No-Action Position Respecting Broker-Dealers Operating Under Fully Disclosed Clearing Agreements According to Certain Functional Allocations (FIN-2008-G002; March 4, 2008), available at http://www.fincen.gov/statutes_regs/guidance/html/fin-2008-g002.html.
15. Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations—Requirement that Brokers or Dealers in Securities Report Suspicious Transactions, 67 FR 44054 (July 1, 2002).
16. Id.

Finally, a firm may use its reasonable business judgment to decide whether to close an account after a SAR filing has been made. It would be prudent for a firm to implement additional monitoring of an account that is the subject of a SAR filing, particularly if numerous SAR filings are involved.[17]

SAR Quality Considerations

Firms are required to file SARs that are complete, thorough, and timely. Some common errors found on SAR-SF forms include: incomplete narratives (e.g., the form does not identify all relevant parties and/or accounts to a transaction), missing identifying information (e.g., account numbers, social security numbers, addresses and telephone numbers), inaccurate information such as applicable dates of suspicious activity (e.g., typographical errors), and including supporting documents as attachments (supporting documents should not be filed with the form). Of course, there may be legitimate reasons why certain information may not be provided in a SAR, such as when a firm does not have the information.

Care should be used to ensure that SARs are completed in a thorough and accurate manner. For instance, a firm should include all known information regarding the person suspected of engaging in suspicious activity and provide a thorough and complete narrative.[18] Inaccurate information on a SAR, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible, thereby undermining the usefulness of the filing. In particular, the SAR narrative section is critical because it is the only area where a firm may explain why the activity was suspicious.

---

17. "As a general rule of thumb, organizations should report continuing suspicious activity with a report being filed at least every 90 days." See The SAR Activity Review Trends, Tips & Issues, October 2000, available at http://www.fincen.gov/sarreviewforweb.pdf.

18. More specific guidance on writing the SAR narrative is available in the FFIEC Manual, Appendix L (SAR Quality Guidance). The FFIEC Manual was prepared by federal banking regulators for banks and bank examiners and is not determinative of broker-dealers obligations; however, it may provide information that is helpful to broker-dealers. Comprehensive guidance is available from FinCEN (Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative) at http://www.fincen.gov/statutes_regs/files/sarnarrcompletguidfinal_112003.pdf.

SEC's Use of SARs Filed by Firms

SEC Enforcement and the Office of Compliance Inspections and Examinations (OCIE) review, in both the enforcement and examination contexts, all new SAR-SF forms that are filed. SARs are reviewed by the SEC for three primary purposes: (i) to identify any information that may relate to existing SEC Enforcement investigations or OCIE examinations, (ii) to identify any ongoing matters that should be referred for a possible new Enforcement investigation or OCIE examination, and (iii) to identify any ongoing securities fraud matters that merit further investigation or examination by the Financial Industry Regulatory Authority or a state or federal law enforcement agency.

The SEC's proactive review of SARs has resulted in a number of new investigations and examinations and has assisted in many active investigations and examinations. These investigations have included matters concerning insider trading, offering frauds, market manipulation, embezzlement of client funds by a registered representative, unregistered broker-dealer or investment adviser conduct, and advance fee schemes. For example, based on information from a SAR review, the Commission filed an emergency enforcement action to halt an alleged ongoing Ponzi scheme and obtained a temporary restraining order that included a substantial asset freeze. In addition, based on a SAR review, SEC staff initiated a cause examination of a broker-dealer to investigate, among other things, whether a firm was attempting to avoid its prime broker's credit limits on trades by cancelling a series of trades in a client's accounts in violation of the Commission's short sale requirements. This examination resulted in a deficiency letter to the firm addressing the firm's failures to ensure the safety of client assets, properly allocate trades, and properly designate discretionary adviser transactions.

SEC Enforcement Actions for Failure to File

The vast majority of firms appear to take their responsibilities to file SARs seriously and expend a considerable amount of resources to diligently file SARs in accordance with their legal obligations. Similarly, promoting compliance with SAR reporting obligations is a Commission priority.[19]

19. Pursuant to federal securities laws, the SEC has the authority to examine broker-dealers, investment companies, investment advisors, and other securities industry participants for compliance with federal securities laws, and to take enforcement action for violations of such laws.

Two recent cases illustrate the Commission's commitment to promoting SAR compliance. In the first case, the Commission charged Park Financial Group, Inc. (Park Financial), a broker-dealer, with playing a role in a pump-and-dump scheme involving pink sheets stock of Spear and Jackson, Inc. (Spear and Jackson) and failing to file a SAR despite obvious red flags.[20] The scheme primarily was operated through three accounts for British Virgin Island companies (unusual for Park Financial) that required the written approval of at least two authorized individuals before a transaction could occur. The CEO of Spear and Jackson, who did not have trading authority, controlled the accounts, which bought and sold only Spear and Jackson stock. The three accounts also transferred large amounts of Spear and Jackson stock to a stock promoter, who was actively promoting Spear and Jackson. During the relevant period, the stock price was sharply increasing. Park Financial and its principal executed more than 200 trades in Spear and Jackson stock for the three accounts, generating approximately $2.5 million in proceeds. Park Financial, among other violations, never reported any suspicious activity and as a result was required to pay a penalty of over $30,000.

In the second case, the Commission sanctioned Ferris, Baker Watts, Inc. (Ferris) for supervisory failures surrounding a scheme to manipulate stock and for failure to file a SAR as required by 31 C.F.R. § 103.19.[21] Failure to file a SAR is a violation of Section 17(a) of the Exchange Act and Rule 17a-8 thereunder. A registered representative of Ferris, a customer and a registered representative of another firm participated in a scheme to manipulate the market for a publicly traded company. The parties acquired shares of the company through various accounts they controlled. After acquiring a significant amount of the public float for the stock, the parties used a number of manipulative trading practices, such as marking the close of the stock, engaging in matched and wash trades, and attempting to artificially create down-bids to suppress short selling. The information about the manipulative practices was made available to senior executives at Ferris through a number of memorandums discussing the manipulative conduct and a recommendation to file a SAR. Ferris, however, failed to

20. In the Matter of Park Financial Group, Inc. and Gordon C. Cantley, Securities Exchange Act Release No. 55614 (April 11, 2007) and Securities Exchange Act Release No. 56902. (December 5, 2007) available at http://www.sec.gov/litigation/admin/2007/34-55614.pdf and http://www.sec.gov/litigation/admin/2007/34-56902.pdf.

21. In the Matter of Ferris, Baker, Watts Inc., Securities Exchange Act Release No. 59372, Investment Adviser's Act Release No. 2837 (February 10, 2009) ("Ferris Order") available at http://www.sec.gov/litigation/admin/2009/34-59372.pdf.

file a SAR relating to the manipulative conduct despite the available information. As a result of this and other violations, Ferris was ordered to pay a civil money penalty of $500,000, in addition to disgorgement payments.

These enforcement cases illustrate that some firms have had serious failings with respect to complying with their SAR obligations. Accordingly, it is useful for all firms to consider how to manage the money laundering and terrorist financing risks posed by their business and to take this risk profile into account when designing SAR monitoring programs.

Suspicious Activity Reviews by Securities Regulators

By Staff of the Financial Industry Regulatory Authority and the Securities and Exchange Commission[22]

In recent years, broker-dealers—and regulators—have dedicated more time and resources to anti-money laundering (AML) compliance. The U.S. Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA)[23] conduct the majority of AML compliance examinations of broker-dealers.

22. This article was prepared by staff from the Financial Industry Regulatory Authority (FINRA) and the Securities and Exchange Commission's (SEC or Commission) Division of Trading and Markets and the Office of Compliance Inspections and Examinations (OCIE), but does not necessarily represent any staff views. The Securities and Exchange Commission, as a matter of policy, disclaims responsibility for any private publication or statement by any of its employees. The views expressed in this document do not necessarily represent the views of the Commission, or the members of the staff of the Commission.

23. FINRA was created in July 2007 through the consolidation of NASD and the member regulation, enforcement and arbitration functions of the NYSE (the consolidation transaction). FINRA operates subject to the oversight of the SEC and is the largest non-governmental regulator for all securities firms doing business in the United States. FINRA is dedicated to investor protection and market integrity through effective and efficient regulation. FINRA oversees nearly 5,000 brokerage firms, about 173,000 branch offices and approximately 656,000 registered securities representatives.

Following the USA PATRIOT Act's amendments to the Bank Secrecy Act, FINRA published NASD Rule 3011, effective April 2002. NASD Rule 3011 requires each member firm to have an AML compliance program in place that is reasonably designed to achieve and monitor the firm's ongoing compliance with the requirements of the Bank Secrecy Act and the implementing regulations promulgated thereunder. The New York Stock Exchange (NYSE) promulgated a comparable rule, NYSE Rule 445, in April 2002, which FINRA incorporated into its rulebook as part of the consolidation.[24] Compliance with NASD Rule 3011 or NYSE Rule 445 also constitutes compliance with the Bank Secrecy Act's AML compliance program requirements.[25]

The SEC and FINRA both examine broker-dealers for compliance with the Bank Secrecy Act and its implementing regulations, as well as for compliance with Rule 17a-8 under the Securities Exchange Act of 1934 (Exchange Act), NASD Rule 3011 and NYSE Rule 445.[26] Each year since 2002, the SEC and FINRA have conducted over 2,000 examinations of broker-dealers that have included an AML review. Even prior to the passage of the USA PATRIOT Act, which expanded the scope of a broker-dealer's AML obligations, FINRA conducted examinations of securities firms for compliance with the AML obligations in place at the time, such as Currency Transaction Reporting (CTR), structuring and the joint and travel rules.

A significant focus of the SEC and FINRA's AML examination programs is on the broker-dealers' policies and procedures to identify and report suspicious activity. These are examined as part of the examiners' review of Exchange Act Rule 17a-8, which requires broker-dealers to comply with the reporting, recordkeeping and record retention requirements of the implementing regulations under the Bank Secrecy Act. They are also examined to ensure compliance with NASD Rule 3011(a), which requires that firms registered with FINRA establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions under 31 U.S.C. 5318(g) and the underlying implementation of those policies and procedures as part of 31 CFR 103.19, which requires broker-dealers to report suspicious transactions.

---

24. The current FINRA rulebook includes (1) FINRA Rules, (2) NASD Rules and (3) rules incorporated from NYSE. For more information about the rulebook consolidation process, see FINRA *Information Notice* 03/12/08 (Rulebook Consolidation Process).

25. See 31 CFR 103.120; see also 31 U.S.C. 1538(h)(1).

26. Throughout this document, NASD Rule 3011 citations have a comparable NYSE Rule 445 citation for members of the New York Stock Exchange.

There are three questions firms most often ask of the securities regulators in connection with examinations of a firm's suspicious activity reporting: (1) what are the examiners looking for when conducting their reviews, (2) will the examiner "second-guess" a decision not to file a Suspicious Activity Report (for the Securities and Futures Industries, or SAR-SF); and (3) what are the examiners finding during their examinations?

Examination Priorities

To address the first question, when conducting an examination for Exchange Act Rule 17a-8, NASD 3011(a) and 31 CFR 103.19, examiners generally focus their review on four items:

1. Written Policies and Procedures – Examiners review the policies and procedures of the firm to see if they are designed to address the risk of the firm's business, such as its size, where its customers and branch offices are located, how accounts are opened, and the types of customers and products handled by the firm. In addition, examiners review procedures to determine whether they address the specific requirements of 31 CFR 103.19, which include the filing of SAR-SFs and the safeguarding of SAR-SF information along with the notification to law enforcement, when required.

2. Implementation of the Written Policies and Procedures – Equally important to having policies and procedures is their implementation. Examiners test the procedures to determine whether the firm is actually following its procedures.

3. Monitoring for Suspicious Activity – Examiners assess whether the firm's transaction-monitoring system and the adequacy of the system, either automated or manual, is reasonably designed to identify potential suspicious activity and whether the firm files SAR-SFs when appropriate. Examiners also review any exception reports used by the firm to monitor activity.

4. Reporting of Suspicious Activity – Examiners review a sample of SAR-SFs that the firm filed to determine the accuracy of the filing, including the timeliness of the filing, whether the firm correctly completed the SAR-SF form, whether the firm maintained proper supporting documentation and whether the SAR-SFs have been kept confidential. In addition, examiners also conduct an independent review for undetected suspicious activity.

Suspicious Activity Reporting

To address the second question, examiners will accept a firm's decision not to file a SAR-SF as long as the firm demonstrates that it had reasonable, risk-based controls and a reasonable decision-making process, and the examiners must find that the firm's decision not to file a particular SAR-SF was reasonable under the facts and circumstances. However, examiners have found that some firms did not implement reasonable, risk-based controls and as a result, they failed to identify transactions showing "red flags" for suspicious activity that were identified in the firm's own procedures.

For example, during one examination, a firm's records showed excessive wire activity and penny stock transactions that indicated the customer might be involved in a market manipulation. The firm did not follow up to analyze these red flags as required by the firm's procedures and, hence, did not file a SAR-SF. In such cases, FINRA and the SEC would likely cite the firm for failing to implement its procedures and may cite the firm for failing to file a SAR-SF.

Common Examination Findings

Regarding the third question about common examination findings, one of the more common findings is that firms fail to have adequate suspicious activity reporting procedures. The procedures are deemed inadequate based on the nature of the firm's business and its clientele. For example, one firm had an online business and customers located in higher-risk jurisdictions, neither of which was addressed in its procedures. In many instances, firms also fail to identify suspicious customer activity and file SAR-SFs where required. For other firms, the procedures failed to set forth the process under which a SAR-SF filing is to be made, how often reviews are conducted, what documents are reviewed, who conducts the reviews, and who within the firm has the authority to make a determination as to whether to file a SAR-SF. Additional findings include the following:

- Failure to document reviews of suspicious activity;
- Incomplete SAR-SF Forms;
- SAR-SFs in which items are completed inaccurately;

- SAR-SFs in which the narrative section fails to adequately describe why the activity was suspicious;
- SAR-SFs that include attachments even though the Form SAR-SF specifically states that supporting documentation should not be filed with the report;
- SAR-SFs not being filed in a timely manner; and
- Inadequate due diligence conducted once potentially suspicious activity is identified; for example, a firm may fail to use readily available public information about a customer's criminal or regulatory history when evaluating potentially suspicious activity for a SAR-SF filing.

More frequently, examiners find that firms have failed to identify and report, as necessary, potentially suspicious transactions involving low-priced securities known as "penny-stocks." The following scenario has been identified on several examinations:

1. Substantial deposit, transfer or journal of very low-priced and thinly traded securities;
2. Journaling of those shares between related and unrelated accounts;
3. Systematic sale of those low-priced securities shortly after being deposited, transferred or journaled into the account;
4. Multiple wire transfers out of the accounts—usually to third parties and many times to offshore tax havens; and
5. Little to no other activity in the accounts other than the deposit of low-priced securities, liquidation of shares and the wiring out of funds.

Transactions like these are red flags for the sale of unregistered securities, and possibly even fraud and market manipulation; they need to be investigated thoroughly by the firm. However, several firms failed to obtain information regarding the source of the stock certificates, the registration status of the shares, how long the customer has held the shares and how he or she happened to obtain them, and whether the shares were freely tradable and no longer restricted resulting in unregistered offerings. Often times, these transactions involve the deposit of physical certificates, which have their own red flags, such as the shares were not issued in the

name of the customer, or were recently issued or sequentially numbered. In several instances, firms did not flag this activity for further review and no SAR-SFs were filed where appropriate.[27] In January 2009, FINRA issued *Regulatory Notice 09-05* reminding firms of their obligations in this area.[28]

Firms have an obligation to report any suspicious transactions "by, at or through" the firm.[29] Examinations have disclosed that some firms review reports that show journals of money, large wire transfers, large money movements and checks distributed from client accounts, but fail to review trading activity or securities movements in order to identify patterns of suspicious activity involving securities. Recent enforcement actions have highlighted the importance of broker-dealers monitoring all aspects of their business and not just money movements.[30] The expectation is for firms to monitor potentially suspicious trading in customers' accounts, as well as the flow of funds and securities into and out of accounts.

Both clearing and introducing firms have independent obligations to review for suspicious activity. Yet, despite this requirement, examiners have found instances where the clearing firms were relying on their correspondent firms who introduce their business to them to conduct suspicious activity reviews, with the clearing firms conducting little to no reviews of their own.[31] Conversely, despite the clearing firm making reports available to its correspondent introducing firms to assist them in their review for suspicious activity, some correspondent introducing firms were not conducting suspicious activity reviews of their own, but rather were relying on their clearing firm to conduct the review.

The monitoring of suspicious activity and the filing of SAR-SFs are cornerstones of any firm's AML program. Broker-dealers should expect examiners to review their suspicious activity reporting program whenever an AML review is conducted.

---

27. *In the Matter of Franklin Ross* (20060046142) (2007); *In the Matter of James I Black and Jess Tucker*, 2006007424601(2008); *See Nevwest Securities Corporation* (E022004011201) (2007), in which FINRA found that the firm's decision not to file a SAR was unreasonable under the circumstances.
28. See FINRA *Regulatory Notice 09-05* (FINRA Reminds Firms of Their Obligations to Determine Whether Securities are Eligible for Public Sale) issued January 2009.
29. See 31 CFR §103.19.
30. *In the Matter of E*Trade Securities LLC and E*Trade Clearing LLC* (2006004297301) (2008); Southwest Securities Inc. (2005002895501) (2008).
31. *Southwest Securities Inc.* (2005002895501) (2008); Wells Fargo Investments LLC (20070073069) (2008).

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), Currency Transaction Reports (CTRs) 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 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 industry involved and type of violation committed.

In many cases, SAR confidentiality requirements preclude FinCEN from associating the name of all law enforcement agencies and entities that utilized SAR information for specific cases highlighted in *The SAR Activity Review*. FinCEN appreciates the help and support of the following agencies and entities that contributed to the cases in this issue: The United States Attorney for the Eastern District of California, ICE, DEA, FBI, IRS, ATF, USPIS, and the Connecticut State Police. Contributing editors: Shawn Braszo, Jennifer White, James Emery, and Jack Cunniff.

In this edition of *The SAR Activity Review*, we take a special look at fraud cases. We review several examples where SARs were used in or triggered investigations centering on the securities industry, traditional Ponzi schemes, and mortgage fraud.

Suspicious Activity Reports help law enforcement agencies investigate fraud cases and prosecute perpetrators in many ways, ranging from focusing complex, time-consuming investigations to paving the way for victims to obtain restitution. Often fraud cases are initiated on the basis of a SAR filing from a financial institution that noticed suspect transactions. In such cases, neither the victims nor law enforcement agencies may have been aware of the criminal activity. Once filed, these SARs are subsequently read by both SAR review teams and individual investigatory agencies, and with the SAR in their possession law enforcement can assess the size and scope of the fraud and investigate the crime, leading to prosecution of the defendants and possible restitution for the victims. Even when a case is not initiated from a SAR, the existence of such a report can provide invaluable leads to investigators.

Cases Involving the Securities Industry

Immigration and Customs Enforcement (ICE) investigated two cases from the securities industry initiated from SARs that had wide impact and claimed many victims. In the first case, the perpetrators set up a boiler-room operation in the United States, but targeted victims in another country. An alert depository institution noted that account activity did not match the firm's stated business activity. In the second case, a securities broker notified U.S. Customs of suspect activity in a filing that originated before that industry had a regulatory requirement to file SARs.

Guilty Pleas in International Hedge Fund Fraud Case Initiated from SARs

An investigation into hedge fund fraud that was initiated from a SAR resulted in guilty pleas, forfeiture, and in the case of the ringleader, a lengthy prison sentence. The prosecution began several years ago when a federal grand jury charged four men in connection with the fraud. All of the victims were non-U.S. residents, and the international investigation utilized FinCEN's 314(a) information sharing process as well as exchanges of information through the Egmont Group of financial intelligence units.[32]

The leader of the scheme, a foreign national, entered the United States on an E-2 Treaty Investor Visa[33] and purported to be operating hedge funds and financial advisement firms which catered to wealthy citizens outside of the United States.

The leader had previously engaged in financial fraud in his home country and received a civil admonition in a non-U.S. court more than ten years ago. In addition to the civil admonition, the defendant received probation and was banned from operating any financial businesses in his home country. Around this time, the defendant came to the United States and started boiler room operations for the fraudulent hedge fund.

---

32. The Egmont Group of financial intelligence units (FIUs) is an international network designed to improve interaction among FIUs in the areas of communications, information sharing, and training coordination. The goal of the Egmont Group is to provide a forum for FIUs around the world to improve support to their respective governments in the fight against money laundering, terrorist financing and other financial crimes.

33. As a treaty investor, the Immigration & Nationality Act provides non-immigrant visa status for a national of a country with which the US maintains a treaty of commerce, who is coming to the US to carry on substantial trade or, to develop and direct the operations of an enterprise in which the individual has invested; or is in the process of investing a substantial amount of capital.

The lead defendant in the fraud utilized his purported hedge fund consulting agencies to sponsor individuals who spoke his native language and were seeking work in the United States. The defendant applied for immigration status for his workers and utilized them as boiler-room operators. These individuals would contact wealthy citizens in the target country through a cold-calling technique and entice them to purportedly purchase stocks in the U.S. market. The operatives used data mining software to collect information from public sources, including individuals' and businesses' names, addresses and phone numbers. The data collected was then entered into a spreadsheet and used to make calls to potential investors.

Once investment funds were received via wire, the funds were transferred among several accounts controlled by the defendant and his co-conspirators. The funds were ultimately spent on personal and business expenses in furtherance of the fraud. Very few stocks were actually purchased with the funds. The defendant instructed his workers on how to use deceptive measures and lies to extract more money from unsuspecting investors. Investors who attempted to cash out their investments were instead persuaded to wire additional funds to meet fictitious withdrawal thresholds and subsequently lost even more money. The total estimated loss was approximately $21 million from over 800 foreign investors.

When investigators interviewed the boiler room operators, the employees revealed that they were not aware of the fraud being perpetrated by the lead defendant. In fact, the defendant held fake board meetings with "board members" in which he also included the boiler room operators. During these meetings, the defendant discussed the stocks the business had invested in and the number of shares held in certain companies.

Two years prior to the indictment, a financial institution filed a SAR on the business and its president (the lead defendant) for a number of suspect activities. According to the SAR, the company's business was solely purported to be an advisor to hedge funds with all income limited to fees from those hedge funds. However, the bank noticed deposits originating from individuals in the target country. In addition, the principals of the company wired funds to companies controlled by the defendant. Finally, the SAR noted that foreign bank regulators had previously closed businesses related to the defendant for various violations, including improper licenses and illegal foreign exchange transactions.

Soon after the financial institution filed the SAR, an analyst with the financial enforcement group of a law enforcement agency identified the filing during a routine review. The analyst conducted further research on the defendant and eventually referred the case to a task force for investigation. In addition to the SAR that identified the financial activity, a SAR filed by a broker-dealer highlighted more than $1 million in questionable wire transfers. That SAR noted that a government office had identified 19 liens and judgments recorded against the defendant's business.

In the course of the investigation, more than $400,000 in victims' funds were recovered and seized from bank accounts. Another $100,000 was seized from brokerage accounts. Investigators identified accounts overseas, including European countries known for their private banking services to non-residents. The lead defendant received a prison sentence of more than 15 years and was ordered to forfeit more than $20 million to be used for restitution to victims of the fraud.

Securities Dealer Provides Details of High Yield Investment Program Scheme

Six defendants pled guilty and received prison time for defrauding investors in a case that started when a securities firm noticed suspect transactions and reported the activity to law enforcement. The defendants created a bogus investment scheme, marketed it over the Internet, and defrauded nearly 200 investors from around the world of more than $16 million.

The case began in 1998 when a task force received a suspicious activity report from a brokerage firm regarding five related accounts. The brokerage firm did not file a SAR with FinCEN, as broker/dealers did not have a regulatory obligation to file SARs at that time, but maintained a close relationship with law enforcement and instead handed a paper document to U.S. Customs. The paper document was subsequently lost in the September 11 terrorist attacks on the World Trade Center in New York City.

An analysis of the accounts and documents in the possession of the brokerage firm, though, indicated that the subject business account was acting as a collection account for millions of dollars that were being sent from locations inside and outside the United States. Once received into this account, the funds were either journal transferred to one of the related accounts or transferred out of the United States. The

funds that were journal transferred to other brokerage firm accounts were transferred out of these accounts to bank accounts in the United States and abroad or used to pay for personal expenses of those involved in the fraud scheme.

The defendants' convictions resulted from their development and orchestration of an elaborate scheme to defraud investors. More than ten years ago, the two primary defendants in the scheme began holding themselves out to investors as promoters of a high-yield investment program that promised massive returns within a short period of time. The defendants created a series of fictitious European banks from which investors were to "lease" funds to invest, normally for a leasing fee of about $35,000. Payment of this fee would purportedly release $1 million, which the defendants claimed would then be placed in the high-yield trading program. In reality, no funds were released and the investment programs were nonexistent.

The defendants pocketed the leasing fees and eventually defrauded victims out of approximately $17 million. As the number of victims increased, and the scheme became more complicated, the defendants recruited subordinates to help maintain the illusion that brokers were recommending the investment programs and that the banks were actual financial institutions. Three of these subordinates pled guilty in the case.

In addition to the plea allocutions, the government's case at trial rested on the voluminous documentary evidence recovered during searches of the defendants' residences, including forged documents used to assure the victims that their "leased" funds were available for investment. Several victims testified, as did foreign and American banking officials who established that the banks created by the defendants were fictitious. Both lead defendants were convicted on all counts.

At the time the business accounts with the broker-dealer were discovered, the total amount collected in the account was approximately $14 million. An additional $2 million was located in a European country. Investigators eventually seized assets worth in excess of $10 million which have been used to make restitution to defrauded victims. The architects of the scheme were convicted in a jury trial of conspiracy, wire fraud, money laundering, and interstate transportation of stolen property; one received a prison sentence of more than 16 years and the other received a sentence of more than 11 years.

Traditional Ponzi Schemes

While some large-scale Ponzi schemes have made headlines in the past few months, similar schemes have been defrauding innocent victims for years. BSA records, particularly SARs, have become an important tool for fighting Ponzi schemes. In this edition, we include three examples of how SARs contributed to the investigations of Ponzi schemes. In the first case, a SAR was the launching point for an investigation. In the next two similar but separate cases, subjects previously apprehended for fraud attempted to pay court-ordered restitution (and steal more money) by creating even more sophisticated frauds. These last two examples highlight the synergy of know-your-customers policies and suspicious reporting. In particular, these cases exemplify how well-researched and well-written SARs ultimately benefit consumers and taxpayers.

SAR Jump-Starts Investigation into Natural Resources Ponzi Scheme

A purported entrepreneur convinced scores of individuals to invest in ventures and businesses supposedly related to the extraction of natural resources that were, in realty, part of a sophisticated Ponzi scheme. The defendant followed a familiar pattern evident in such schemes: paying earlier investors with funds from new investors as well as keeping a substantial amount for himself. When victims first complained about the defendant, law enforcement had little information on him and few leads. Around the same time that victims were contacting law enforcement, a financial institution also filed a SAR on a suspect transaction. When victims made subsequent complaints, agents located the SAR and launched a full-scale investigation that resulted in an arrest within a few months.

The scheme ran for about 5 to 6 years, with the defendant generally promising to double investors' money within one year. In all, he raised about $10 million from about 100 investors. The defendant memorialized the investors' loans in a series of promissory notes and security agreements, in which he pledged as collateral the various natural resources to be extracted from property that he leased. He flagrantly overstated the value of the collateral as he tried to induce prospective investors. Contrary to his promises that he would use the funds for various business-related purposes, he in fact used a substantial portion of the money he raised to make partial payments to earlier investors and to support a lavish personal lifestyle.

The defendant was arrested and charged in the scheme and while on pre-trial release improperly tried to solicit more money from investors. All together, three banks where the defendant held accounts filed SARs on suspicious transactions. Many of the transactions listed in the SARs directly led to the charges included in the complaint and indictment. The SARs describe how the defendant frequently asked his investors to write checks to third parties, claiming that they were only to show new investors that the ventures had financial backing. However, the defendant frequently cashed or deposited these checks.

A federal judge sentenced the defendant to more than 10 years in prison following his guilty plea to counts of mail fraud, wire fraud, bank fraud, and money laundering. The presiding judge ordered that he serve five years of supervised release following completion of his prison term and pay restitution totaling almost $10 million.

Bank SARs Lead to Discovery of Predatory Certificate of Deposit Fraud Scheme

In order to satisfy fines and restitution ordered as a result of an earlier scheme, two defendants began a new multi-state advertising campaign scheme to attract buyers (mostly elderly) of non-existent certificates of deposits.

As part of the scheme, one of defendants rented office space in one state and hired workers to handle investor inquiries. He also established a mail drop in a distant city to receive investor payments. The mail drop in that city had instructions to forward all mail to a second mail drop in yet another state. Investors mailing payments to that mail drop were told to make the checks payable to another company that was actually a shell company. To convert the investor payments into personal cash, the second defendant opened a series of shell bank accounts. After reviewing transactions related to the accounts, the bank filed a SAR and notified law enforcement.

The bank SAR that initiated the case noted that one of the defendants opened accounts for several businesses that ultimately turned out to be fronts for the fraud scheme. The bank noticed that checks made out to one business were deposited into the account of another business. In addition, the bank believed the transactions in the account were indicative of fraud because there appeared to be no discernable legitimate business activity, only small monthly payments to individuals that appeared to be interest payments.

The SAR narrative described critical elements of the crime in detail. The bank noted that the age of the investors ranged from approximately 60 to 90 years of age, and the checks had notations on the memo lines consistent with the purchase of Certificates of Deposit. The withdrawals from the account were in the form of checks made out to cash in amounts ranging from $4,000 to $9,500. And, as indicated, the only activity in one account was small monthly checks to individuals.

Bank staff asked numerous questions of one of the defendants, and his responses reinforced their fears that he operated a predatory fraud scheme aimed at senior citizens. The bank froze one of the accounts with a balance of almost $400,000. The defendant responded with only a cursory protest and said he would contact his lawyers. The bank explained the circumstances to the defendant's lawyer but the defendant took no further action in the matter.

Law enforcement and prosecutors noted that the SAR proved instrumental in ending the scheme and the funds in the frozen account provided restitution for some victims. The two defendants were sentenced for their roles in the scheme. One received a 30-year prison sentence in exchange for a guilty plea for his role in the two fraud schemes. In addition, he was ordered to pay almost $5 million in restitution. The severity of the sentence, unusual for white-collar crime with a plea agreement, stemmed from the defendant's role as leader in both schemes as well as his refusal to account for the stolen funds. His co-defendant also pled guilty and received a sentence of more than 7 years.

Bogus Life Insurance Investment Vehicles Identified through SAR Filing

The defendants in this case first settled a civil suit with the government concerning the sale of $7 million worth of fraudulent "prime-bank" note investments to investors nationwide. In the scheme, investigators found that less than half the money was used to pay fictitious investment returns to existing investors. The rest was used by the perpetrators of the fraud for personal expenditures.

The defendants then orchestrated a Ponzi scheme in which they solicited more than $60 million from dozens of investors, according to court documents. The pair told investors that their money would be used to purchase pools of life insurance policies on behalf of an organization. In return, a small portion of the death benefit would go to the family of the insured, but the majority of the money would be paid back to the defendants' company. Investors were promised they would receive a high annual return and were told their "risk-free" investments would eventually yield a five-to-one return.

Prosecutors charged that only a fraction of the funds were used to purchase two pools of life insurance policies, and that approximately $60 million was used by the defendants to further their lavish lifestyles, including the purchase of houses, cars, boats, and jewelry. One defendant also transferred approximately $10 million in investor funds to an unrelated business venture.

The investigation into the Ponzi scheme started with a SAR filed by a depository institution. The SAR narrative described how, during routine due diligence in the wake of the press reports concerning the original government action on the prime bank guarantees, the filing institution realized that the defendants had a number of accounts at the institution. One account had more than $15 million in unusual transactions credited to it in a three-month period.

An agent investigating the case noted that the SAR proved "absolutely crucial" to the success of the case. Because of the filing, law enforcement was able to unravel the scheme quickly. In less than a year, and from a reported $1 million in losses, agents uncovered more than $60 million in fraudulent transactions resulting in the indictment and arrests of the subjects. Moreover, additional BSA filings on the subjects helped agents find assets that were seized for restitution.

Mortgage Fraud Cases

FinCEN has reported on the increase in the number of SARs that cite mortgage fraud as a potential violation.[34] Law enforcement uses these SARs to investigate and prosecute mortgage fraud cases, two of which are recounted here. In the first case, depository institutions filed SARs on both the defendant's business and personal accounts. When the lead investigator identified these SARs, he established a close working relationship with the institutions which facilitated the flow of information necessary for a quick arrest of the subject. In the second case, the extra effort on the part of the depository institution in developing information on a defaulting mortgage holder helped identify a mortgage fraud ring.

34. See Mortgage Loan Fraud Connections with Other Financial Crimes and Filing Trends in Mortgage Loan Fraud. Additional information on Mortgage Fraud is available on FinCEN's website, www.fincen.gov.

Case for Mortgage Fraud Involving Straw Buyers Supported by SARs

BSA records helped identify co-conspirators, accounts, and elements of a mortgage fraud scheme that may total as much as $7 million dollars in losses. SAR filings described transactions related to the fraud in both personal and business accounts belonging to the defendant in the case, and CTRs filed by a bank and a money services business identified currency transactions that were consistent with fraudulent activity.

In a scheme that lasted for approximately three years, the defendant and his co-conspirators profited by selling residential real estate in the Mid-Atlantic area to individuals acting as straw buyers. The defendant and his co-conspirators, through a business the defendant established, helped the straw buyers obtain 100% mortgage financing to purchase the properties. To obtain the mortgage financing, the conspirators produced fraudulent loan applications that included materially false statements related to the buyers' employment, income, immigration status, and intent to occupy the properties as primary residences. The straw buyers frequently defaulted on these mortgages, causing losses to banks and commercial lenders in excess of $2,500,000.

During the period that the fraud was being perpetrated, several banks filed SARs noting unusual patterns of activity. SARs filed on the defendant's business note that the applicants for the loans may have overstated employment and inflated salaries, lied about the use of the home as a primary residence, or provided other information that created discrepancies indicative of mortgage fraud. SARs filed on the defendant's personal accounts highlighted patterns of structured withdrawals as well as cashier's checks that were cashed in a manner consistent with fraudulent behavior.

Investigators who reviewed the SARs reached out to the respective banks for more information on the defendant and his co-conspirators. The banks continued to monitor the accounts closely, filed additional SARs, and simultaneously notified the lead investigator. A bank noted in one SAR that certain suspect transactions involving official checks did not appear to serve any logical business or personal reason. The bank also noted as unusual the receipt of wires and checks from title companies into a personal account by an individual who has a mortgage lending business.

A federal judge sentenced the defendant to more than five years in prison, followed by supervised release, and ordered him to pay several million dollars in restitution.

Proactive Suspicious Activity Report Review Leads to Guilty Pleas in "Cash Back" Mortgage Fraud Scheme

In a case that started from a proactive review of Suspicious Activity Reports, a specialized mortgage fraud task force launched an investigation that led to charges against two individuals. Bank Secrecy Act records captured many of the scheme's intricate details, including a SAR filed on one of the defendants who was described as being "very upset" when he learned that a CTR would be filed as a result of a series of transactions.

According to the assistant United States attorney who prosecuted the case, the indictment charged that over an 18 month period the defendants engaged in a scheme to defraud mortgage lenders in connection with residential real property purchases. The leader of the scheme recruited various individuals, including straw and nominal purchasers, to purchase more than a dozen real properties. In addition, the leader orchestrated the transactions and conspired with a mortgage broker to complete the fraud.

The indictment charged that the transactions involved fraudulent or false representations in obtaining 100% mortgage financing, including misstatements about the purchasers' monthly income, intent to occupy the property, and existing liabilities. In addition, the indictment alleged that in each transaction the purchase price was above the true market price of the property. An amount approximately equal to the difference between the purchase price and the true market price was diverted as "cash back" at the close of each escrow into the bank account of an out-of-state corporation. As part of the scheme, the defendant caused these credits to be concealed from the mortgage lenders. The indictment charged that the defendant in fact exercised control over the out-of-state corporation bank account and used the fraudulently obtained funds for various purposes, including extensive cash withdrawals.

The case originated after a SAR review team identified a SAR filed on one of the straw buyers, an associate of the defendant. Because the SAR listed mortgage loan fraud as the suspected violation type, the team referred the SAR to a mortgage fraud task force. The SAR filer noted that the subject (the aforementioned straw buyer) apparently misrepresented information on a loan application for a mortgage that was in default. The co-conspirator and mortgage broker acted as the loan agent and broker of record on the loan. Through research, the filing institution found that the subject had purchased four additional properties for which each mortgage loan totaled at least $490,000. All properties were closed by the same title company.

Investigators identified several additional related SARs, including one with a lengthy narrative describing activity on 18 individuals and businesses associated with the scheme. Investigators included many of the details described in the SARs in a criminal complaint and as evidence in the indictment charging the defendant and co-conspirator. One SAR noted that a co-conspirator became irate when he learned that a CTR filing was required following a series of transactions.

The original criminal complaint described in detail the defendant's efforts to defraud lenders through straw buyers. While the defendant approached the buyers to invest in properties and open bank accounts, he actually controlled all aspects of the purchases and the accounts. Although the buyers provided the defendant with truthful personal information, the defendant made false representations on the loan applications in regard to income, employment, and intent to occupy the residences.

In late 2008, the leader of the mortgage fraud scheme pled guilty to mail fraud and structuring currency transactions at a financial institution to evade the reporting of the transactions. The total losses in the fraud exceeded $2.5 million.

Investigating agencies include Federal, State agencies and Local Police Departments.

Section 4 - Issues & Guidance

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

On March 3, 2009 FinCEN announced a Notice of Proposed Rulemaking on the Confidentiality of Suspicious Activity Reports. Also on March 3, FinCEN proposed Interpretive Guidance on the sharing of suspicious activity reports by securities broker-dealers, mutual funds, futures commission merchants and introducing brokers in commodities with affiliates that are also subject to SAR rules. The Notice of Proposed Rulemaking and the proposed Interpretive Guidance were posted to the Federal Register on March 3, and financial institutions are encouraged to provide written comments, which may be submitted to FinCEN through June 8, 2009.

Identifying and Reporting Suspicious Transactions for Introducing and Clearing Broker-Dealers

By FinCEN Office of Regulatory Policy

Since the passage of the USA PATRIOT Act and the promulgation of enhanced requirements for the securities industry, there has been significant attention focused on the anti-money laundering requirements of introducing and clearing broker-dealers.

In the securities industry, it is common for "introducing" firms to enter into arrangements with "clearing" firms that establish the responsibility of each firm with respect to functions required to be performed, from opening the account to sending confirmations and statements to the customer. These clearing agreements, which are done pursuant to the rules of a self-regulatory organization, most typically allocate to the introducing firm the responsibilities for opening and approving accounts and taking and receiving orders. The clearing firm most commonly takes on the responsibilities for extending credit, executing and settling transactions, safeguarding funds and securities, and issuing confirmations and statements.

With respect to AML compliance, introducing and clearing brokers generally have independent responsibilities. In March 2008, FinCEN issued a no-action position with respect to the requirements under the Customer Identification Program Rule. FinCEN has also addressed obligations of clearing firms with respect to the Correspondent Account and Private Banking Rules under section 312.[35] In addition, the Financial Industry Regulatory Authority (FINRA) has issued certain information since the passage of the USA PATRIOT Act addressing the SAR reporting obligations of introducing and clearing firms.[36]

Key Points for Suspicious Activity Reporting

1. The obligation to identify and report a suspicious transaction rests with each broker-dealer involved in a transaction.

    - Both introducing and clearing brokers have independent obligations to monitor account activity for suspicious transactions.

    - Introducing and clearing firms may coordinate their activities to detect suspicious activity to allow each firm to meet its obligations to comply with its SAR requirements.

        - Introducing firms may be in better position to monitor activity in connection with opening the account and communicating directly with the customer. Clearing firms may be in a better position to monitor customer transaction activity, including for example trading, wire transfers and cash movements into and out of the account.

35. See *Application of the Regulations Requiring Special Due Diligence programs for Certain Foreign Accounts to the Securities and Futures Industries*, FIN-2006-G009 (May 10, 2006).

36. See NASD Notice to Members 02-21 (April 2002) and FINRA Small Firm Template (Last updated January 23, 2004), available at http://www.finra.org/Industry/Issues/AML/P006340.

- In some situations, clearing firms may be able to develop tools or enhance existing tools which might assist introducing brokers in analyzing the transactional activity of its customer.

2. Introducing brokers and clearing firms may develop effective communication procedures that permit coordination when questionable activity or potential indications of suspicious activity are detected by either firm.

   - Introducing and clearing firms involved in a transaction may share information about that particular suspicious transaction for purposes of determining which firm will file a SAR.

   - Introducing and clearing firms involved in a transaction may opt to file a joint SAR-SF, but the report must include all relevant facts covering the transaction or pattern of transactions. The purpose of this provision is to allow two broker-dealers that have participated in the same transaction or pattern of transactions to file only one SAR. However, each firm involved in the joint filing must maintain supporting documentation on the SAR filing.

   - Firms should remember that the disclosure limitations found in 31 U.S.C. 5318(g)(2) on dissemination of the SAR, and disclosure of the fact of its filing, apply equally to both broker-dealers that are jointly filing a SAR.

   - The introducing broker and clearing broker may have separate criteria for evaluating the transactions and may make different determinations as to whether a suspicious activity report is required to be filed. In cases where a SAR is not jointly filed, the filing institution may not disclose to the other broker that a SAR has been filed.

   - Introducing and clearing firms may file notices under the Section 314(b) safe harbor to share information that may involve possible terrorist or money laundering activities, as permitted for all financial institutions complying with the 314(b) rule. Such information sharing may allow firms to identify and report activities that may involve terrorist acts or money laundering and to determine whether to open or maintain an account or engage in a transaction. Firms should note, however, that although information shared under the 314(b) program enjoys the benefit of safe harbor protection, the 314(b) safe harbor does not cover the disclosure of a SAR or information indicating that a SAR has been filed. Firms must, therefore, abide by the rules governing SAR confidentiality.

Broker-dealers that are either introducing or clearing firms should remember that each has independent responsibilities to identify and report suspicious activity. While introducing and clearing firms may allocate certain monitoring functions in a fully disclosed clearing agreement,[37] this does not alter their separate and distinct obligations under the SAR rule. For example, when a clearing firm is not allocated the responsibility of monitoring customer accounts according to the terms of a fully disclosed clearing agreement, it nonetheless is obligated to establish policies, procedures, and controls that are reasonably designed to detect and report suspicious activity that is attempted or conducted by, at, or through it, including activity that is introduced to it by another firm.[38] Moreover, firms may develop effective communication procedures when potential indications of suspicious activity are detected to ensure that each firm is able to satisfy its suspicious activity reporting requirements.

SAR Form Completion When Reporting Identity Theft

By FinCEN Office of Regulatory Policy

Identity theft occurs in many forms and can include additional crimes of false statement, computer intrusion, credit or debit card fraud, mortgage loan fraud, or wire transfer fraud. As a means of better identifying and tracking known or suspected criminal violations of identity theft, a financial institution should report identity theft and any additional suspicious activities involved on a SAR. In situations involving multiple violations of law, reporting identity theft in conjunction with additional suspicious activities can be of significant assistance to law enforcement. This serves to notify law enforcement of the nature of the activity and may be valuable to law enforcement personnel in seeking a greater awareness of an entire pattern of activity.

37. NYSE Rule 382 and NASD Rule 3230 (permitting clearing and introducing firms to allocate regulatory and operational functions between them, including the responsibility for opening, approving and monitoring accounts; extending credit; maintaining books and records; receiving and delivering funds and securities; safeguarding customers funds and securities; issuing trade confirmations and account statements; and accepting orders and executing transactions).

38. See 31 C.F.R § 103.19(a)(2).

It is important that the SAR narrative contain a full picture of the suspicious activity involved. The narrative should be a chronological and complete account of the possible violation of law. For example:

- A suspect accesses the victim's investment account via the internet using the victim's name and account information and places trades for all of the securities in the account. The suspect then attempts to wire the proceeds to a bank account in a foreign country. The broker-dealer becomes aware of the identity theft after contacting the victim to verify the unusual account activity and the unusual destination of the wire transfer.
- A suspect establishes an investment account with a broker-dealer via the internet using the victim's personal information and attempts to wire funds from the victim's bank account. The account activity appears legitimate. The broker-dealer becomes aware of the identity theft only when informed by the victim's bank that the transfer of funds is unauthorized.

The SAR narrative should include information about the suspect (if available), how the account was accessed, if the attempt involved an online virus (e.g., a trojan or spyware) and what instruments or mechanisms were used in the transaction(s). The narrative should also include the accounts involved, the date and period of time the suspicious activity took place, whether the attempt appears duplicative and frequently occurred in different customer accounts, the place the activity occurred, whether a foreign jurisdiction was involved, whether another financial institution was involved, how the identity theft was detected, and why the activity is suspicious.

Further, it is important to note that all filers should ensure that they have provided as much detail as possible in the narrative regarding the suspect and activities involved in the identity theft. Unless the victim is suspected to have contributed to the identity theft scheme, the victim is not a suspect. If suspect information is unknown or unavailable, any partial or incomplete identifying information should be included. For example, a suspect through a trojan online-virus obtains personal information of the victim, contacts the victim's bank by phone and submits a notice of a change in address and requests for a new or additional debit/credit card. The filer when completing the narrative may be able to provide the suspect's address and phone number used to contact the bank.

Alternatively, the suspect information may be unknown or unavailable. For example, a suspect using the victim's personal information may attempt a transaction, such as a funds transfer at the victim's bank, but when asked for identification cannot provide

authenticating information and terminates the transaction. In these instances, the financial institution should include whatever identifying information is available (email address, description, etc.) in the narrative.

Global Resolution of Potential Enforcement Actions

By FinCEN Office of Enforcement

A broker-dealer, mutual fund, or futures commission merchant in violation of requirements to implement adequate measures reasonably designed to ensure compliance with the Bank Secrecy Act (BSA), including detection and reporting of suspicious activity indicative of money laundering, terrorist financing, or other financial crimes, may be subject to enforcement actions by multiple government agencies.[39] FinCEN may assess civil money penalties against a broker-dealer, mutual fund, or futures commission merchant for violating the BSA.[40] In addition, the U.S. Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), or U.S. Commodity Futures Trading Commission (CFTC) may also take enforcement action, under their respective jurisdictions,[41] for violations of counter-money laundering requirements similar to, but separate from, the BSA.

When charged with conduct violating the BSA and other counter-money laundering requirements, a broker-dealer, mutual fund, or futures commission merchant should consider seeking global resolution of all potentially related enforcement matters. While the SEC, FINRA, CFTC, and FinCEN must operate under their distinct jurisdictional authorities, we strive, whenever possible, to proceed jointly and concurrently on enforcement matters. Global proceedings advance disposition of BSA enforcement matters in the context of other related matters, and avoid potential for multiple actions against a financial institution at different times for similar or related conduct. In addition, global enforcement actions advance consistent and uniform enforcement of the BSA and other counter-money laundering requirements by all stakeholder government and self regulatory organizations.

39. See U.S. Government Accountability Office, Bank Secrecy Act, Federal Agencies Should Take Action to Further Improve Coordination and Information-Sharing. GAO-09-227 (February 2009).

40. 31 U.S.C. § 5321 and 31 C.F.R. § 103.57.

41. See e.g., Securities Exchange Act of 1934 sections 21B and 21C.

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.

Ensuring Effective Broker-Dealer SAR Programs

By Alan E. Sorcher and R. Stephen Ganis[42]

Notwithstanding all of the USA PATRIOT Act rules that broker-dealers are required to comply with, suspicious activity monitoring and reporting remains at the heart of a firm's compliance program. While the SAR rule is far from new, firms must ensure that their program is kept current and relevant. Failure to do so can put a firm at risk of missing detectable suspicious activity and, potentially, violating the BSA. The spate of allegations stemming from the financial crisis about illegal activity in the securities markets, moreover, presents an opportunity for broker-dealers to review the scope and methodology of their suspicious activity detection and reporting practices.

42. At the time of writing this article, Alan E. Sorcher was General Counsel of the Bankers Association for Finance and Trade. R. Stephen Ganis is Of Counsel at the law firm of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. Both authors have served on the U.S. Department of the Treasury Bank Secrecy Act Advisory Group and various sub-committees thereof.

Background

One of the biggest challenges of the SAR rule is the wide net that it requires firms to cast. The rule, in general, requires the reporting to FinCEN of any "suspicious transaction relevant to a possible violation of law or regulation" of at least $5,000 in funds or other assets that is conducted or attempted by, at, or through the broker-dealer. Broker-dealers should remember that securities law violations are covered. The rule allows firms to follow a risk-based approach in monitoring for suspicious activity. Firms are expected to "evaluate customer activity and relationships for money laundering risks and design a suspicious transaction monitoring program that is appropriate . . . in light of such risks." Thus, a firm can fashion a SAR program that makes sense for its business so long as it appropriately addresses the suspicious activity risks inherent in that business.

A difficult aspect of risk-based SAR programs is that the risks confronting broker-dealers are constantly changing. The events of the past year have demonstrated that things are often not what they seem and firms should pay careful attention to the widening range of transactions that might be deemed to pose suspicious activity risks. Types of transactions by, at or through broker-dealers that were thought to pose little or no risk of suspicious activity a year ago may, when analyzed in light of intervening events, be found to pose increased risks today. With that in mind, here are some basic points to help keep your SAR program up to speed.

Addressing Current Events and Emerging Trends

Financial Crisis

The current financial crisis, which resulted in two significant impacts on broker-dealer suspicious activity detection and reporting practices, has shown that financial institutions must try to be prepared for the unpredictable.

First, the crisis has changed the nature, size and volume of transactions that need to be monitored for potential suspicious activity. Systems and processes using customer profiles and rule parameters based on pre-existing notions of "normal" transaction sizes and volumes may need to be adjusted to reflect current market realities. Indeed, enormous movements and volatility in the markets over the past year have made it more difficult for firms to use stock price or volume swings to help identify suspicious activity.

Second, the crisis has revealed suspicious activity risks that might not have been apparent before. Firms should therefore pay close attention to current events and emerging risks and, when appropriate, incorporate them into their SAR program. Recent cases demonstrate vulnerabilities to suspicious activity in transactions with or on behalf of even those customers with top reputations. Just as the crisis has highlighted the potential vulnerability of the lending industry to mortgage fraud, it has similarly highlighted the vulnerability of the brokerage industry to securities fraud and manipulation. For example, federal regulators have alleged widespread manipulative short sales and credit default swaps trading by certain kinds of institutional customers of broker-dealers. Regulators in other countries have responded to similar allegations in foreign markets by issuing guidance clarifying that potentially manipulative short sales are subject to mandatory suspicious transaction reporting by market intermediaries. The crisis has also highlighted risks associated with certain custody arrangements, for example risks arising when institutional customers act as their own custodian without appropriate safeguards. Therefore, broker-dealers may wish to evaluate the extent to which recent allegations and revelations in the current financial crisis might impact the risk assessment underlying their suspicious activity detection practices.

Cyber Crime

Broker-dealer SAR programs should appropriately address the rapidly escalating threats posed by cyber crime. The potential harm to financial institutions in this area is significant. Particularly relevant to broker-dealers are several cases the SEC has brought involving online brokerage accounts, in particular with fraud relating to account compromise. The schemes typically combine electronic intrusion into online brokerage accounts with traditional market manipulation. A typical manipulative scheme involves traders hacking into investors' online accounts, selling the investor's securities positions, and using the proceeds to purchase shares of stocks subject to the scheme in a way that artificially inflates their price. Another common scheme involves theft from compromised accounts through electronic funds transfers. While these cases may be more relevant to firms that permit customers to transact online, they should not be ignored by the rest of the industry. Cyber crime continues to grow and firms should be on alert for red flags that may signal that something is amiss.

Trade-Based Money Laundering

While historically more of an issue for banks, broker-dealers increasingly need awareness about trade-based money laundering. Because of the increasing focus by banks and their regulators on the trade-based money laundering threats arising in traditional letter of credit financing, there is a danger that laundering through trade might migrate to non-banking financial institutions. Thus, broker-dealers processing frequent or large cross-border payments, especially wire transfers, should consider evaluating their vulnerability, if any, to trade-based money laundering red flags. Trade-based money laundering can occur through under- or over-invoicing or routing several invoices through various financial institutions, leading to multiple payments for the same goods. There have also been cases where the quantity, quality and type of goods and services have been misrepresented, or where the shipping and customs documents differ from what is actually shipped. As participants in illicit trade finance grow more sophisticated about evading the intensifying scrutiny, it has become increasingly difficult to assess the genuineness of international trade transactions. Thus, broker-dealers with a large international presence may, depending on their business model, need to review whether necessary measures addressing emerging trade-based money laundering threats, if any, are necessary.

Reported Suspicious Activity

A SAR program should address current suspicious activity events and emerging trends not only within the broader securities markets generally, but also within the firm itself. Much can be gained from firms taking full advantage of actual suspicious activity they have reported, evaluating select SAR filings for broader trends and reviewing enforcement actions. All of these may be an excellent source of training and red flags that some firms may not be utilizing to the extent possible. Firms may need to make changes in their systems in response to reported suspicious activity. Names mentioned on SARs may aid in monitoring and customer due diligence. In addition, applying resources to evaluating SAR filings for broader trends may have significant benefit. Firms may be able to identify similar schemes, common locales or names, or possible red flags. Last, broker-dealers should follow enforcement actions involving securities fraud or manipulation occurring through brokerage accounts and relationships, and BSA and criminal money laundering violations more generally. These can reveal vulnerabilities that need to be addressed and areas of concern for the regulators.

Identification and Analysis of Transaction Types

One challenge associated with implementing an effective SAR program is identifying all the types of transactions "by, at or through" a financial institution that are potentially subject to SAR filing requirements. This challenge is particularly pronounced for broker-dealers because typically more kinds of transactions occur in a brokerage account than in, for example, a demand deposit account. In addition to the full range of cash management and payment transactions associated with most bank accounts, brokerage accounts often permit a wide range of securities investment and trading activities. Most securities transactions are covered by the definition of "transaction" applicable to a SAR filing and include a "purchase or sale of any stock, bond, … or other … security … or any other payment, transfer or delivery by, through or to a financial institution, by whatever means effected." This definition is broad enough to capture not just monetary transactions (e.g., wire transfers, check deposits and disbursements, bill payments, automated clearinghouse and other electronic funds transfers, and other "cash" transactions) but also securities transactions, including purchases, sales, certificate of deposits, full and partial automated customer account transfers, free deliveries and receipts, external withdrawal by transfers, and internal journal entry transfers. Recent FINRA enforcement actions demonstrate compliance risks presented when a broker-dealer's suspicious activity monitoring and detection efforts do not focus sufficiently on those securities transactions that are not accompanied by monetary transactions.

It may be a worthwhile exercise for a broker-dealer to go periodically through each type of transaction processed in the accounts it introduces or carries, whichever applies, to confirm the extent to which:

- suspicious activity detection systems or processes in place address the risks posed by the transaction type in each relevant business line; and
- any additional suspicious activity detection measures that may be necessary.

Because the universe of transaction types offered or processed by broker-dealers changes frequently, a transaction-by-transaction analysis of suspicious activity detection measures and gaps may need to be updated over time. In particular, business and operational changes such as automation of manual processes, migration of transaction processing from one systems environment to another, and roll out of new products or services may change the universe of transactions subject to SAR filing requirements that occur "by, at or through" a particular broker-dealer.

Identification of Detection Points

Another ongoing practical challenge for a broker-dealer in maintaining an effective SAR program is ensuring that the anti-money laundering officer or unit coordinates sufficiently with all points in its organizational structure that might detect or otherwise become aware of potential suspicious activity that could require a SAR filing. This means that potential suspicious activity may need to be escalated not just by employees who handle SAR compliance but also by other departments. In this connection, broker-dealers may wish to review individuals or teams that handle the following types of matters to validate that they are, where necessary, incorporated adequately into escalation workflows:

- identity theft, account compromise, true name fraud, and check fraud;
- insider trading, market manipulation and other securities fraud;
- matches between customer accounts and information sharing requests sent to the broker-dealer through FinCEN pursuant to Section 314(a) of the USA PATRIOT Act;
- law enforcement and regulatory subpoenas;
- customer tax issues;
- customer due diligence (regulatory/disciplinary history, etc.);
- credit reviews of customer relationships and trading activity;
- operations (branch, treasury/cashiering, purchase/sale, foreign securities, restricted securities, physical deposits, and safekeeping);
- interactions with other firms concerning customer account activity; and
- employee financial crime or prohibited trading.

Conclusion

Maintaining an effective SAR monitoring and reporting program poses challenges for firms, and the recent market disruptions have increased those challenges. However, the compliance and reputation benefits for firms being able to root out potential wrongdoing at an early stage are quite apparent – and can be accomplished through a rigorous and flexible surveillance program that reflects emerging suspicious activity threats in an unusually dynamic capital markets environment.

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. 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

__ **Dealers in Precious Metals, Precious Stones, or Jewels**
__ **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 - 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?

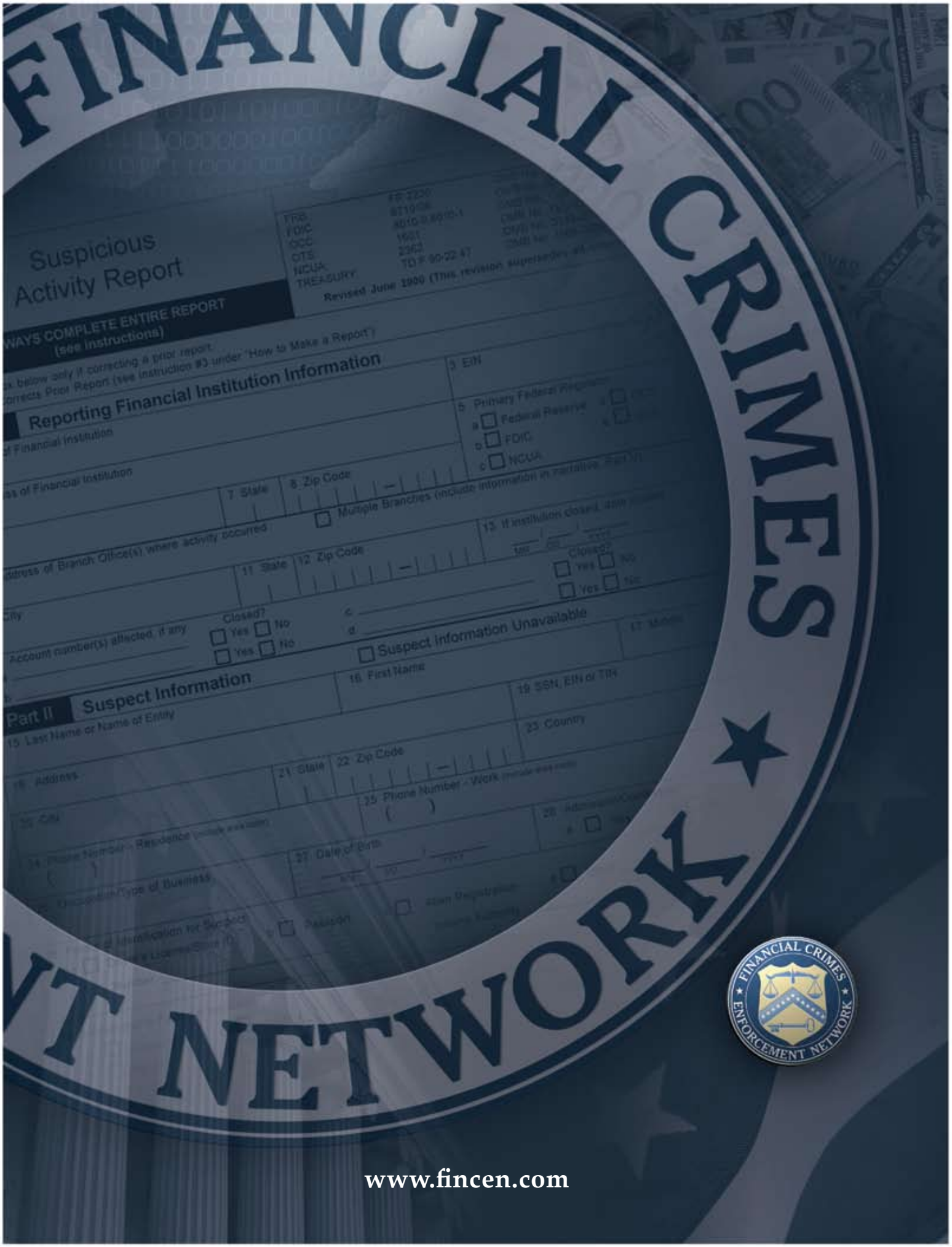
_____
_____
_____
_____

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

[ ] 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

The *SAR Activity Review* **Index** is now 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



www.fincen.com