The SAR Activity Review

Trends Tips & Issues

Issue 23

Published under the auspices of the BSA Advisory Group.
May 2013

Financial Crimes Enforcement Network

The SAR Activity Review

Trends Tips & Issues

Issue 23

Published under the auspices of the BSA Advisory Group.
May 2013

Table of Contents

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

Introduction

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

The *Trends & Analysis* section of this issue opens with an article on SAR filing patterns related to elder financial exploitation before and after the publication of FinCEN Advisory FIN-2011-A003 (*Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation*) in February 2011. In this section we also report on trends related to SAR filings involving accountants and involving insider abuse within depository institutions. We close this section with an article from FinCEN's Office of Special Programs Development on how financial institutions have made use of, and benefited from, information sharing under Section 314(b) of the USA PATRIOT Act.

The *Law Enforcement Cases* section includes interesting and informative summaries of cases that demonstrate the importance and value of BSA data to the law enforcement community. Cases in this section highlight how BSA data, and the detection and analysis of suspicious transactions by financial institutions, proved to be of value to law enforcement and prosecutors.

The month of May is Older Americans Month, and in the *Issues & Guidance* section we include a message from the Consumer Financial Protection Bureau (CFPB) on efforts by CFPB, FinCEN and others to raise awareness of elder financial exploitation. In this section, we include an additional article with information beneficial to filers of the new FinCEN SAR: *SAR Narrative Key Terms: Updated Guidance on the Use of SAR Check Box Items*.

Finally, in the *Industry Forum*, we get feedback from industry recommending the inclusion of a check box on the FinCEN SAR for reporting human trafficking.

As always, we very much appreciate your feedback. Please take a moment to fill in the form at the end of this issue to let us know if the topics we have covered are helpful to you, as well as what you would like to see covered in future editions.

Barbara Bishop
Regulatory Outreach Project Officer
Financial Crimes Enforcement Network

The SAR Activity Review – Trends, Tips & Issues is possible only as a result of the extraordinary work of many FinCEN employees and FinCEN's regulatory, law enforcement and industry partners. FinCEN would also like to acknowledge the members of the Bank Secrecy Act Advisory Group (BSAAG) SAR Activity Review Subcommittee for their contributions to the development of this publication, particularly the Co-chairs noted below.

Helene Schroeder
Special Counsel
Commodity Futures Trading Commission

[OPEN]

Trends & Analysis

This section of *The SAR Activity Review – Trends, Tips & Issues* contains trend information, such as those identified through analysis of FinCEN reports and through information sharing under Section 314(b) of the USA PATRIOT Act.

Update: Elder Financial Exploitation

By FinCEN's Office of Regulatory Analysis

In February 2011, FinCEN issued FIN-2011-A003 (*Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation*).[1] The advisory provides SAR filers a list of red flags that may potentially signal elder financial exploitation and specifically requests that filers include the term "elder financial exploitation" in the narratives of relevant SAR filings. The purpose of the Advisory was not only to help institutions detect suspected elder financial exploitation and report it using a standardized term; it was also to highlight how an institution's ongoing efforts to fight elder financial exploitation can complement its AML program.

Filing Trends

A comparison of the filing rates pre and post-advisory of SARs with narratives containing the two key search phrases "elder financial exploitation" and "elder financial abuse,"[2] shows a very significant increase in relevant filings post-advisory. Between March 1, 2011, and August 31, 2012, filers submitted 7,651[3] total SARs, a 382 percent increase from the 12-month period prior to the release of the advisory

1. See the Advisory, http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2011-a003.pdf.
2. Although the advisory did not specifically instruct filers to use the latter term, FinCEN wanted to insure identification of all relevant SARs and thus included the additional phrase in the search.
3. These results include 6,026 suspicious activity report filings submitted by depository institutions (SARs), known as legacy SARs, 1,183money services business filings (SAR-MSBs), 352 securities and futures industries filings (SAR-SFs) and 90 new unified SAR filings (FinCEN SARs). In March 2012 FinCEN began to accept voluntarily-filed unified SARs (FinCEN Form 111). FinCEN's new SAR (and CTR) is designed to accommodate the different types of industries that will file this report. As such, the new SAR contains certain suspicious activity characterizations generally relevant to a specific industry. FinCEN located no casino and card club filings (SAR-Cs) that met the search criteria for this report.

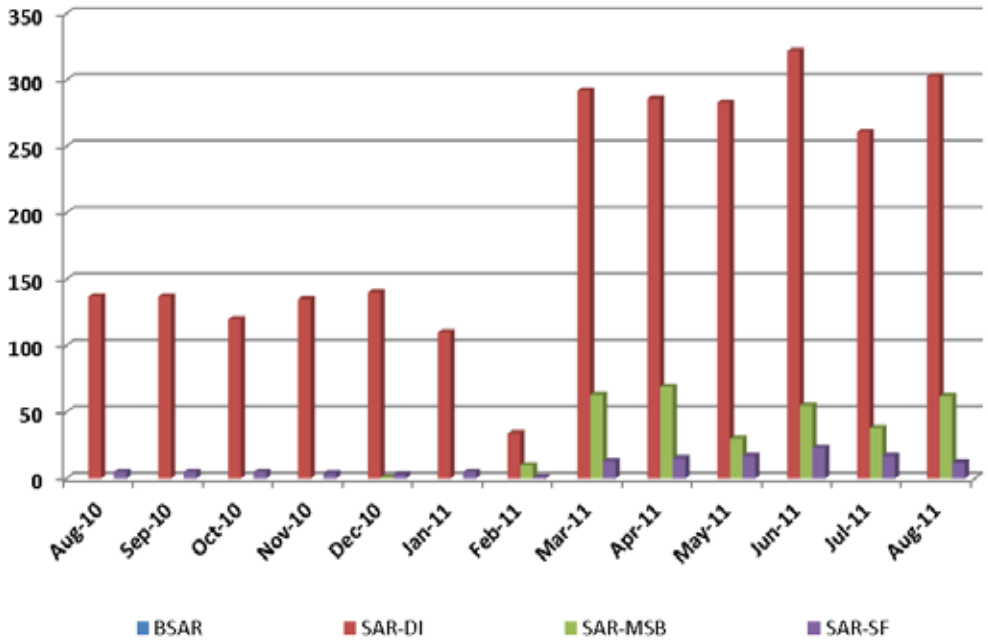
during which filers completed 1,589 relevant SARs. Post-advisory filing trends showing continued increases in filing incidences suggest that many filers have incorporated the relevant FinCEN guidance into their Bank Secrecy Act/Anti-Money Laundering (BSA/AML) suspicious activity and risk monitoring programs.

SARs generally reported patterns of financial exploitation perpetrated by a relative or caregiver against elderly victims. Narratives most frequently described the perpetrator coercing or cajoling the victim into completing financial transactions that benefited the perpetrator at the expense of the victim. In other instances, the perpetrator reportedly abused his/her power of attorney over the victim's account. Filers of SAR-MSBs most often reported unusual wire activity by their elderly customers, including multiple same-day wire transfers, sometimes from different agent locations, to different cities in the United States, as well as unusual wires to moderate and/or high-risk countries. These filings generally described the elderly customer falling victim to some type of scam. One particular sample SAR-SF detailed activity commonly referred to as a "sweetheart scam."[4]

Chart 1 provides an overview of filing patterns six months before and six months after release of the advisory. Not counting the month FinCEN issued the advisory (February 2011), during the six-month period just prior to the advisory, filers submitted 806 filings (779 SARs, 1 SAR-MSB, and 27 SAR-SFs) compared to 2,161 (1,747 SARs, 317 SAR-MSBs, and 97 SAR-SFs) filed during the six-months following the advisory. Of special note is the increase in SAR-MSBs post advisory.

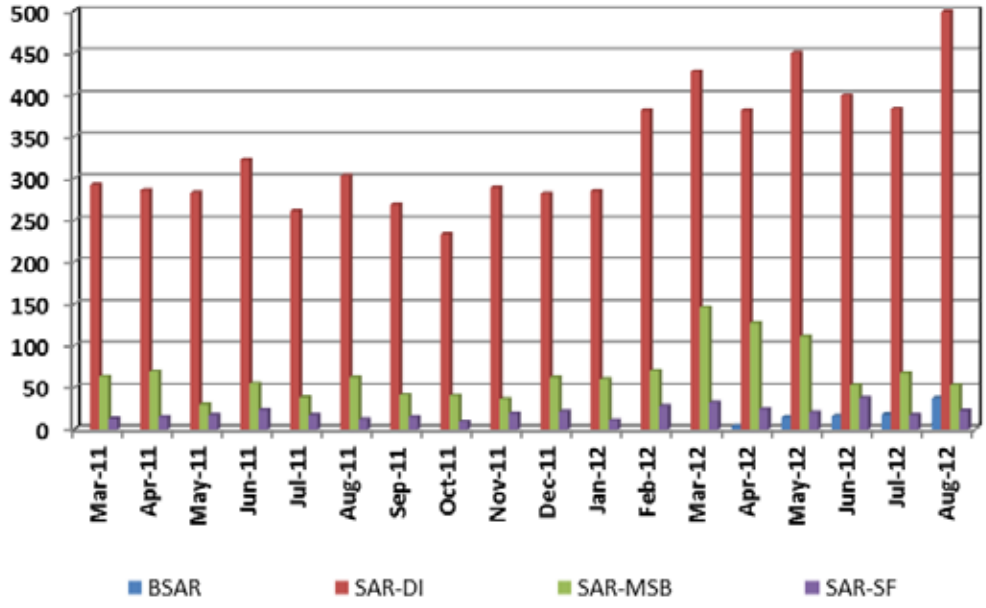
4. A "sweetheart scam" involves the fraudster feigning romantic intentions towards a victim, thus gaining the victim's affection. The perpetrator then uses the goodwill engendered to defraud the victim. This fraud may impact the victim's financial accounts and/or identity security, and may even cause the victim to unwittingly facilitate financial fraud against others on the perpetrator's behalf.

Chart 1
Elder Financial Exploitation Filings
(August 2010 – August 2011)



Though it is not uncommon for relevant filings to increase in the period just after the release of an advisory, during the 18-month post advisory period (March 2011 through August 2012), the number of filings citing elder financial exploitation continued to trend higher. Chart 2 displays the 18-month post-advisory filing activity. This sustained trend upward suggests that many filers have incorporated FinCEN's elder financial exploitation guidance into their suspicious activity and risk monitoring programs.

Chart 2
Elder Exploitation Filings
18-Month Look Back



Depository Institutions filed 6,026 elder financial exploitation-related SARs in the 18 months post-advisory. In reviewing a representative sample of SARs, depository institution filers identified "abuse by a relative or caregiver" as the most reported characterization of suspicious activity, followed by "other suspicious activity types" that facilitated the financial exploitation, including identity theft, misuse of position or self-dealing, embezzlement/theft/disappearance of funds, check fraud, check kiting, and counterfeit debit/credit card.[5]

During the same period MSBs filed 1,183 elder financial exploitation SARs. MSBs commonly reported structuring as the characterization of suspicious activity, including the same individual(s) using multiple locations over a short time period, altering a transaction to avoid completing a funds transfer record for transactions of $3,000 or more, or two or more individuals working together. MSBs also reported multiple types of fraud, including wire transfer, securities, mail, credit/debit card and check fraud. Filers reported elderly customers who were victims of scams, including lottery fraud, and various types of consumer fraud. In addition,

5. FinCEN also identified 90 relevant BSA/Unified Reports (BSAR FinCEN Form 111) filed during the same review period.

narratives described fraudsters trying to appeal to an elderly person's sense of compassion by relating fabricated stories describing the immediate financial needs of a fraudster's purported relative in medical distress or legal trouble. In most cases the MSB caught the activity, blocking transactions when it believed an elderly customer was not aware that he/she was falling victim to a probable scam.

Filers in the securities and futures industries reported elder financial exploitation in 352 reports during the review period, detailing abuse of elderly clients involving forgery, check fraud, suspicious documents or ID presented, wire fraud, identify theft, embezzlement/theft, and mail fraud.

Summary

Monthly post-advisory filing numbers indicate that filers continued to increase their submissions of SARs related to elder financial exploitation more than a year and a half after issuance of the advisory. This trend suggests that many filers have incorporated FinCEN's elder financial exploitation guidance into their BSA/AML monitoring programs. Sample narratives showed filers checked "Other" most often as the characterization of suspicious activity when describing suspicious transactions involving elderly customers. Most narratives described the perpetrator engaged in identity theft, misuse of position or self-dealing, check kiting, counterfeit checks, or embezzlement/theft, to defraud elderly victims. Many SAR narratives revealed that filers were careful to assess suspicious transactions, often questioning an elderly customer if his transactions appeared out of character. These precautions usually spared the filer and the customer any significant losses.

SAR Assessment: Abuse of Insider Relationships within Depository Institutions

By FinCEN's Office of Regulatory Analysis

FinCEN analysts recently conducted research and analysis to identify the extent and methods of insider abuse as reported in depository institution Suspicious Activity Report (SAR-DI) filings submitted on the legacy report[6] between January 1, 2003 and June 30, 2012. Analysts also collaborated with law enforcement partners to obtain general views of the value of Bank Secrecy Act (BSA) information in prosecuting insider abuse cases, and with regulators to determine efforts to prevent or identify insider activities when they occur, and the institution's actions when discovering such activity. This article is intended to convey information about these efforts and to provide typologies observed in SAR narratives.

Attention to insider abuse activities within financial institutions is high, and insider abuse-related criminal prosecutions have increased. The FBI's most recent *Financial Crimes Report to the Public*, released in March 2012, notes that while a majority of bank failures in recent years resulted from declining market conditions, insider abuse remains a factor, "particularly through participation by bank officers and directors in the wave of mortgage loan fraud activities in the middle of the past decade."[7]

6. Legacy SAR refers to TD F 90-22.41, the form that depository institutions used to report suspicious activity prior to implementation of FinCEN's new SAR form. In March 2012, FinCEN began to accept voluntarily-filed unified SARs (FinCEN Form 111). FinCEN's new SAR (and CTR) is designed to accommodate the different types of industries that will file this report. The legacy depository institution SAR had 20 specific characterizations of suspicious activity in Part III, Item 35 plus an "other" field for filers to describe types of reported activity. The new FinCEN SAR, also sometimes referred to as the BSAR, expands suspicious activity information options to more than 70, allowing financial institutions to provide more detailed information on the type of suspicious activity they are seeing. The new form still allows filers to check the "other" box, but it also includes a text field for the filer to provide additional information. As such, the new SAR contains certain suspicious activity characterizations generally relevant to a specific industry. Financial institutions were required to utilize the new FinCEN reports, including CTRs and SARs, by April 1, 2013.
7. Federal Bureau of Investigation, Financial Crimes Report to the Public, March 1, 2012.

Furthermore, while regulators have long been interested in identifying the methods and extent of insider abuse,[8] they have also consistently found that economic downturns were seldom the sole cause of bank failures, and that management and insider abuse also played a significant role in the failures.[9]

Methodology

FinCEN analysts conducted BSA database research to identify SAR-DIs filed between January 1, 2003 and June 30, 2012, in which filers noted subjects as having insider relationships. Analysts then filtered the results by the types of relationships identified in the SAR-DI form.

Analysts conducted statistical research on the full data set to determine the types of insider relationships, as well as characterization of suspicious activity categories. Analysts then reviewed the narrative sections of a random sample of 384 SAR-DIs for specific trends and patterns, or behaviors that raised red flags and prompted filers to submit the reports.[10] The 384 SAR-DIs reported a total of 544 insider relationships.

Expanded research revealed varying degrees of insider abuse in financial institutions, spanning from egregious instances involving personal benefit, to inadequate oversight or internal controls that enabled management, other employees or principals to expose their institutions to excessive risk. Other data and resources consulted in this review and analysis included:

- Laws, regulations and regulator guidance relating to fraud and insider abuse;
- Compliance and enforcement actions by bank regulators for insider abuse;
- Post-closing reviews of institution failures prepared by bank regulators and their Offices of Inspectors General;
- Indictment and prosecution data in criminal and civil liability prosecutions for losses or institution failures resulting from abusive activities; and
- Law enforcement, industry and government reports and data relating to insider abuse activities resulting in losses and/or insolvency of financial institutions.

8. Minimum Security Devices and Procedure, Reports of SARs, and BSA Compliance Program, Final Rule, 61 FR 4332 (February 5, 1996) (codified at 12 CFR 21). "The OCC notes that insider abuse has long been a key concern and focus of enforcement efforts . . ."
9. General Accounting Office, Bank Insider Activities: Insider Problems and Violations Indicate Broader Management Deficiencies, GAO/GGD-94-88, March 30, 1994.
10. The sample size provides a confidence level of 95 percent with a confidence interval of plus or minus 5 percent.

Research and Analysis

What is Insider Abuse?

The specific term "insider abuse" is not defined in the BSA, but appears in SAR rules issued by Federal financial regulators. For example, regulations of the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC) and National Credit Union Administration (NCUA) require banks to file SARs on insiders, for "insider abuse involving any amount . . . and the bank has a substantial basis for identifying one of its directors, officers, employees, agents or other institution-affiliated parties as having committed or aided in the commission of a criminal act, regardless of the amount involved in the violation."[11] The term "institution-affiliated party" is further defined as "any director, officer, employee, or controlling stockholder (other than a bank holding company) agent, shareholder, independent contractor (including attorney, appraiser, or accountant) . . . who knowingly or recklessly participates in the conduct of the affairs of an insured depository institution."[12]

The General Accounting Office[13] (GAO) reported that absent a "universally agreed upon definition of the term 'fraud and insider abuse' it would adopt the term as defined in a 1988 Federal Home Loan Bank Board (FHLBB) Report to Congress:[14]

" . . . individuals in a position of trust in the institution or closely affiliated with it have, in general terms, breached their fiduciary duties; traded on inside information; usurped opportunities or profits; engaged in self dealing; or otherwise used the institution for personal advantage. Specific examples of insider abuse include loans to insiders in excess of that allowed by regulation; high risk speculative ventures; payment of exorbitant dividends at times when the institution is at or near insolvency; payment from the institution funds for personal vacations; automobiles, clothing and art; payment of unwarranted commissions and fees to companies

11. See 12 CFR 208.62 (Board of Governors of the Federal Reserve System); 12 CFR 353 (Federal Deposit Insurance Corporation); 12 CFR 748 (National Credit Union Administration); and 12 CFR 21.11 (Office of the Comptroller of the Currency).
12. See 12 USC 1786(r), 1813(u) and 1818(b) (3), (4,) or (5).
13. Known since 2004 as the Government Accountability Office.
14. General Accounting Office, Thrift Failures – Costly Failures Resulted from Regulatory Violations and Unsafe Practices, GAO/AFMD-89-62, June 1989. "In a sample review of 26 failed thrifts between 1985 and 1989 "indications of fraud or insider abuse existed at all these failed thrifts." The report cited fraud and insider abuse as "the most pernicious of all factors leading to the insolvency of thrift institutions."

owned by a shareholder; payment of consulting fees to insiders or their companies; use of insiders' companies for association business; and putting friends and relatives on the payroll of the institutions."[15]

Other published definitions include:

- Self-dealing, undue dependence on the bank for income or services by a board member or shareholder, inappropriate transactions with affiliates, or unauthorized transactions by management officials. "Insider" refers to principal shareholders, directors, executive officers, and other officers or staff who, as a result of their position, are able to influence operations or decisions within a bank.[16]
- A general term that encompasses various activities which may or may not be lawful. While an abusive situation usually violates one or more banking laws or regulations, legal violations are not a necessary element. Insider abuse includes the broader range of actions where an insider takes action or fails to take action; where the bank is harmed, takes on additional risk, or loses an opportunity; and where the insider or a related party somehow benefits because of his position.[17]
- "Insider abuse is abuse that falls short of being a criminal act.[18] It occurs when an insider (as defined by Regulation O)[19] benefits personally from some abusive action he/she takes as part of his/her position at the bank. Not all insider violations are necessarily abusive; the violation must be accompanied by personal gain to the insider to be considered abusive. Insider fraud is a criminal act. Such action includes embezzlement, falsifying documents, and check kiting."

---

15. Id. - Citing Federal Home Loan Bank Board Resolution 88-133 (date not provided), in which the Bank Board adopted a staff report describing the actions the Bank Board had taken or planned to take to prevent thrift insolvencies. The resolution also directed the staff to transmit the report as required by the Competitive Equality Banking Act of 1987 to the Congress.
16. OCC, Bank Failure – An Evaluation of the Factors Contributing to the Failure of National Banks, June 1988.
17. Id.
18. GAO/GGD-94-88, March 30, 1994. Furthermore, financial institutions, like any other business, can be vulnerable to financial harm and other misdeeds by their own insiders. Over the years, bank regulators, lawmakers and other government entities have consistently sought to reduce that vulnerability in the banking industry. The OCC Handbook on Insider Activities notes that "a corporate culture of ethical and honest behavior, as well as effective board oversight and management supervision, is a bank's primary defense against insider abuse and fraud." Insider Activities, Comptroller's Handbook (2006), page 4. Available at: http://www.occ.gov/publications/publications-by-type/comptrollers-handbook/_pdf/insideractivities.pdf.
19. Federal Reserve Regulation O provides that loans to bank insiders (officers, directors, and principal shareholders) must be made on the same terms available to regular bank customers. 12 CFR 215.

- Unlike insider abuse, insider fraud does not have to benefit the individual perpetrating the crime. For example, if a bank president falsifies loan documents to improve the apparent creditworthiness of a borrower, this is fraud – even if no personal gain by the president can be identified."[20]

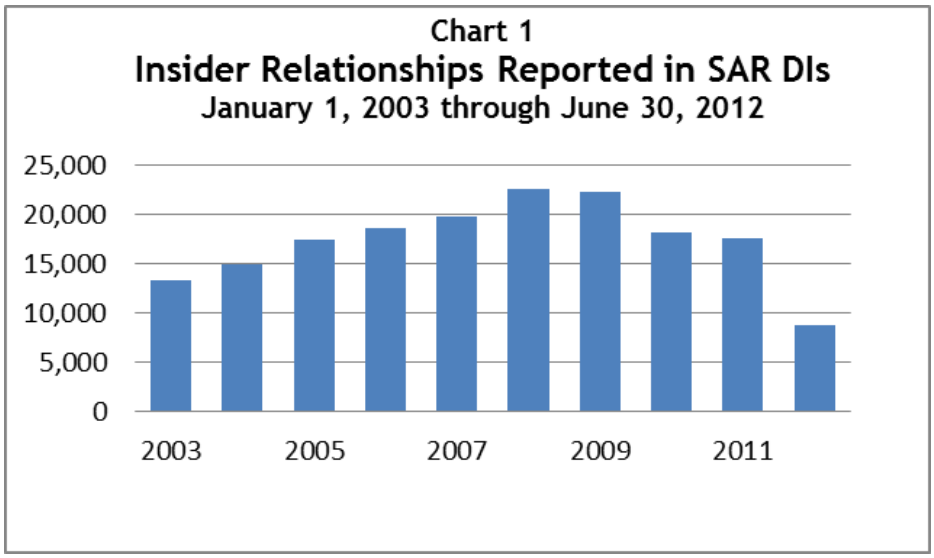
BSA Research and Analysis

Between January 1, 2003 and June 30, 2012, depository institutions reported 201,910 insider relationships in Item 30 (Relationship to the Financial Institution). As shown in Table 1 and Chart 1, insiders as subjects of SAR-DIs rose steadily between 2003 and 2009, after which the reporting volume declined.

Table 1: Annual SAR-DIs Reporting Insider Relationships

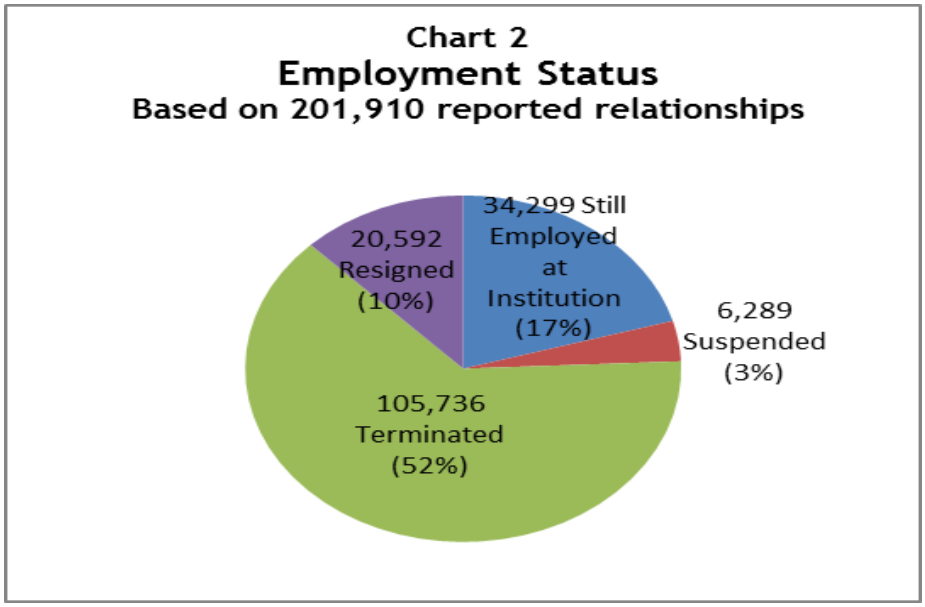
YEAR	*2003*	*2004*	*2005*	*2006*	*2007*	*2008*	*2009*	*2010*	*2011*	*2012**
TOTAL SARs	14,468	16,330	19,154	20,473	22,518	25,782	26,748	22,483	22,163	11,791

***through June 30, 2012**

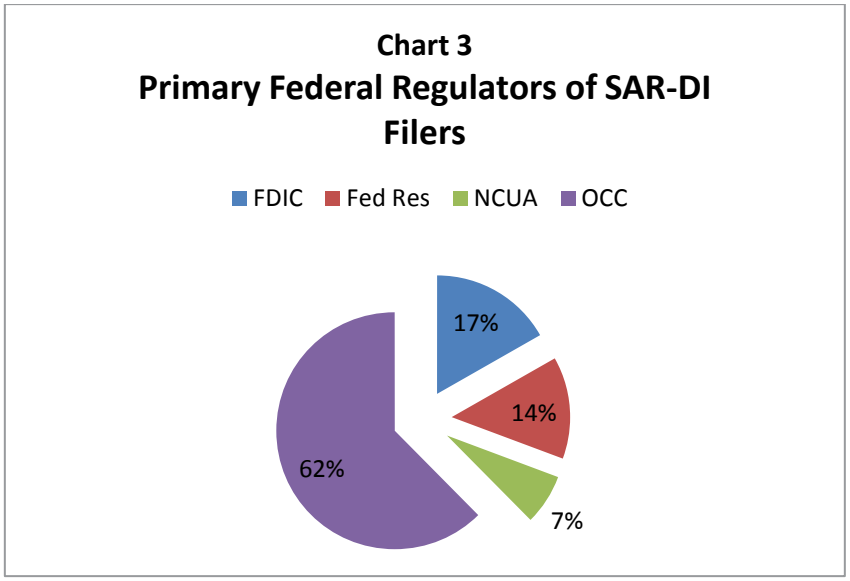


The reporting institution terminated or suspended more than half of the reported insider relationships (55 percent) while 10 percent of the suspected personnel resigned. Conversely, a seemingly significant 17 percent retained their employment. However, some of the insider types identified on the SAR, such as borrower or shareholder, are not categories with actual employment status that can be terminated by a filer.

20. GAO, Report to Congressional Requesters, Bank Insider Activities: Insider Problems and Violations Indicate Broader Management Deficiencies, GAO/GGD-94-88, March 30, 1994. Available at: http://gao.gov/assets/160/154234.pdf.



As shown in Chart 3, the OCC regulated the majority of the filing institutions reporting insider relationships.



Relationship Types

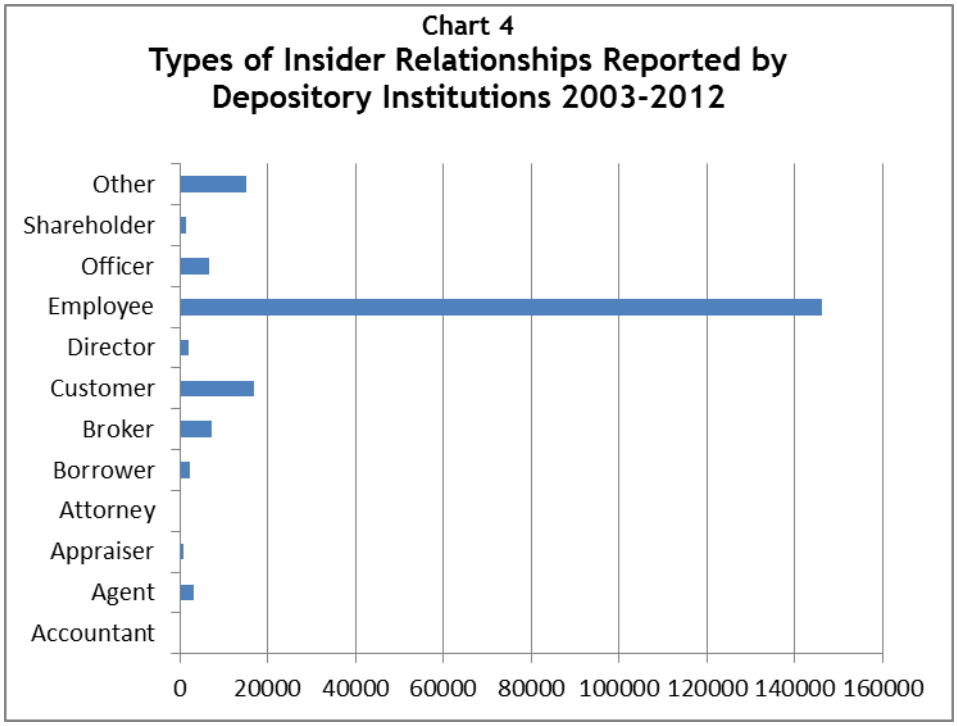
Table 2 and Charts 4-5 illustrate the types of insider relationships identified in each year of this analysis. Chart 5 shows the percentages of the top five types of insiders identified. At 72 percent, the category "employee" far surpassed any other type of insider subject in this analysis. The next highest percentage of insider subjects was "other" at 7 percent. Filers described subjects reported in this

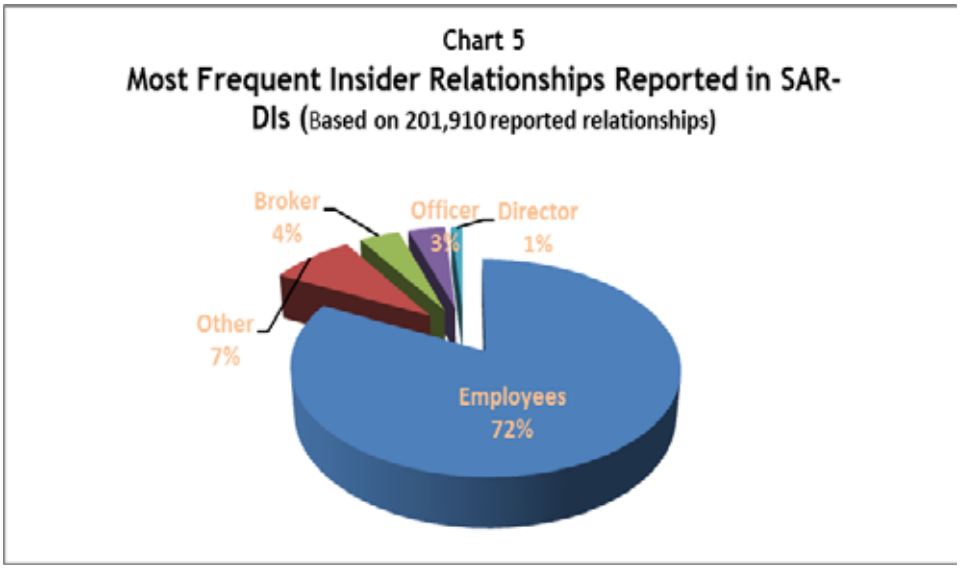
category as former employees, relatives or friends of current or former employees, and employees of the filer's subsidiaries such as mortgage or insurance companies or third-party vendors, among others. Loan applicants were also sometimes reported in this category.

Table 2: Annual Breakdown of Reported Insider Relationships in SAR-DIs

YEAR	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012*	TOTAL*
Accountant	31	28	29	34	21	11	9	12	9	1	185
Agent	121	350	505	375	395	571	447	89	170	81	3,104
Appraiser	6	4	15	19	76	51	348	213	115	28	875
Attorney	9	3	14	11	8	5	19	10	7	3	89
Borrower	105	93	123	134	364	633	321	231	227	158	2,389
Broker	40	46	82	157	378	857	2,510	1,914	921	378	7,283
Customer	1,163	975	1,291	1,242	1,680	1,889	2,229	2,189	2,564	1,673	16,895
Director	142	154	162	151	137	157	279	321	355	182	2,040
Employee	11,395	12,962	14,981	16,456	17,028	19,174	17,605	14,445	14,535	7,521	146,102
Officer	585	656	667	598	662	755	773	813	780	377	6,666
Shareholder	115	76	68	62	74	88	163	191	268	172	1,277
Other	756	983	1,217	1,234	1,695	1,591	2,045	2,055	2,212	1,217	15,005
TOTAL	14,468	16,330	19,154	20,473	22,518	25,782	26,748	22,483	22,163	11,791	201,910

***through June 30, 2012**





Officer and Director Insider Relationships

Table 2 shows a steady downward trend in reported annual insider relationships from 26,748 in 2009 to 22,163 in 2011 (the last full year of this assessment), a 17 percent decrease. Together, reports on officers and directors total four percent of the relationships over the period of this review, a seemingly low percentage overall.

This relatively small percentage of reports on officers and directors is consistent with government experience indicating that insider fraud and abuse by directors, officers and controlling shareholders is not frequently reported in SARs, for a variety of reasons. In a review of institution failures in 1990 and 1991, the GAO found that examiners were not as effective in identifying insider problems in open banks as were investigators after the banks had failed.[21] They made a distinction between examiners whose primary concern is a bank's safety and soundness, with investigators who are concerned about culpability of anyone associated with the bank. Thus they approach their duties differently.

The GAO reported that examiners of open institutions face a wider variety of obstacles that post-closing investigators do not face. For example, examiners are provided with only selected documents and records, and officials involved in abusive or fraudulent conduct often conceal their activities. The GAO concluded that, other than recordkeeping required by Regulation O regarding loans to insiders, the bank's

21. GAO, Bank Insider Activities: Insider Problems and Violations Indicate Broader Management Deficiencies, GAO/GGD-94-88. Available at: http://www.gao.gov/assets/160/154234.pdf.

systems may lack data identifying an insider as a party to a transaction. Also, former bank employees are likely to be more willing to talk to investigators about insider problems after a bank has failed and their jobs are no longer in jeopardy.

A 2012 government-sponsored study conducted by Carnegie Mellon University's Software Engineering Institute on insider fraud in the U.S. financial services, specific to cyber threats, reiterated this fact. That study found that employees may be reluctant to report their supervisors when they violate rules, especially rules that seem to have little association with malicious or criminal conduct. Employees may also be fearful of losing their jobs.[22]

This analysis shows that, overall, SAR-DIs reporting insider relationships decreased during the period of this study. While officers and directors represent a seemingly small 5 percent of the total subjects in the dataset, a closer look at the statistics shows that filings on directors actually increased slightly during the review period by 34 SARs. Filings on officers increased from 773 in 2009 to 813 in 2010, but declined back to 780 in 2011, for a net increase of 7 SARs. Consequently, despite the probable under reporting of insider activities by officers and directors inherent in the industry, the filings on those insiders increased during the period of this review.

SARs reporting insider activities may not provide a comprehensive accounting of all improper financial misdeeds by directors and officers; however, those that are made nonetheless provide invaluable assistance to successful law enforcement investigations and prosecutions.

22. Insider Fraud in Financial Services, Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector, CERT, Insider Threat Center at Carnegie Mellon University's Software Engineering Institute, 2012.

Activity Types

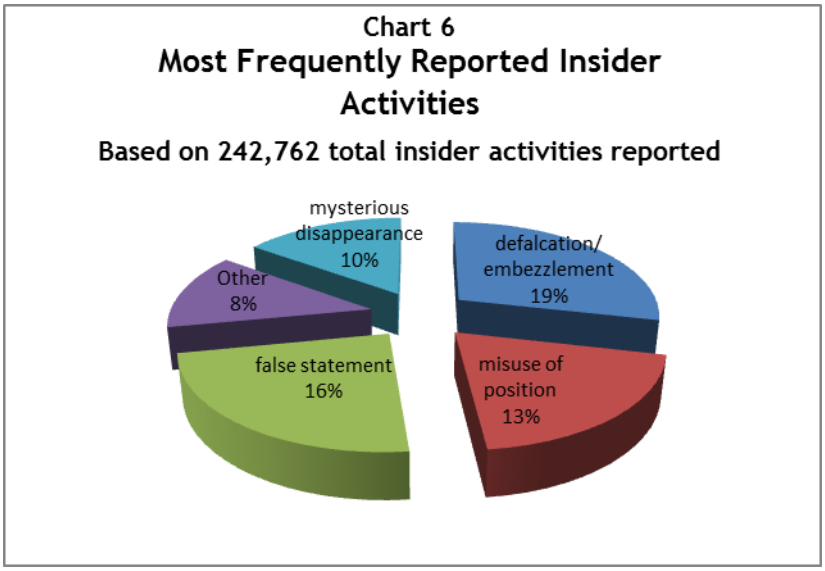
Table 3 provides an annual breakdown of all the activity types reported in these SARs. Note that some SARs may have reported more than one type of suspicious activity.

Table 3: Annual Breakdown of Reported Activity Types

Type of Suspicious Activity	*2003*	*2004*	*2005*	*2006*	*2007*	*2008*	*2009*	*2010*	*2011*	*2012**	**Total***
Bribery/gratuity	80	102	112	149	120	147	99	89	132	46	**1,076**
BSA/structuring/ money laundering	652	746	1,029	1,105	1,378	1,428	1,519	1,488	1,729	838	**11,912**
Check fraud	1,142	962	1,295	1,484	1,566	1,824	1,604	1,271	1,457	733	**13,338**
Check kiting	632	808	880	974	969	945	840	755	625	309	**7,737**
Commercial loan fraud	155	216	190	228	405	762	379	356	332	172	**3,195**
Computer intrusion	146	137	148	164	164	161	117	139	118	46	**1,340**
Consumer loan fraud	409	414	519	568	658	889	496	461	335	261	**5,010**
Counterfeit check	137	137	215	241	194	233	149	114	162	35	**1,617**
Counterfeit credit/ debit card	21	12	20	17	11	19	7	9	10	5	**131**
Counterfeit instrument (other)	61	56	44	80	56	88	88	65	33	25	**596**
Credit card fraud	563	743	828	719	452	506	476	339	265	127	**5,018**
Debit card fraud	179	144	204	261	308	356	308	273	249	171	**2,453**
Defalcation/ embezzlement	4,475	4,804	5,221	5,602	5,650	5,920	5,078	4,160	4,166	2,057	**47,133**
False statement	1,719	1,698	2,011	2,182	3,094	4,254	5,009	4,882	5,081	2,775	**32,705**
Identity theft	57	291	509	678	992	1,133	922	755	915	520	**6,772**
Misuse of position or self-dealing	2,603	3,168	3,955	4,665	4,567	5,633	5,076	3,908	3,720	1,779	**39,074**
Mortgage loan fraud	269	446	685	1,013	1,481	1,739	3,853	3,219	2,365	1,014	**16,084**
Mysterious disappearance	1,821	2,233	2,740	2,809	2,766	2,722	2,250	1,628	1,549	898	**21,416**
Other	1,819	1,975	2,387	2,491	2,749	3,095	3,141	2,630	2,896	1,757	**24,940**
Terrorist financing	9	8	4	2	1	2	2	2	3	3	**36**
Wire transfer fraud	57	85	48	73	105	131	114	219	238	109	**1,179**
Total	17,006	19,185	23,044	25,505	27,686	31,987	31,527	26,762	26,380	13,680	**242,762**

***through June 30, 2012**

Chart 6 depicts the top 5 reported activities associated with insider abuse.



Activity Trends and Patterns in the Most Frequently-Reported Relationships[23]

Employees

Filers associated employees-as-subjects with all five most frequently reported activity categories. Typologies of some of those activities included:

- Teller theft from cash drawer or vault, often followed by forced balancing;
- Misappropriation of customer funds by tellers and other employees by altering deposits, accessing customer funds, or using customer credit to purchase items;
- Fraudulent or empty envelope deposits to the ATM, followed by cash withdrawals;
- Corporate credit card fraud;
- Structuring;
- Check Kiting;
- Opening new accounts for fraudulent or non-existent customers in order to qualify for performance goals or employee incentive programs;

23. All percentages provided in this analysis are based on the complete dataset. Trend(s) and pattern(s) typologies were derived from an analysis of the full narratives in the sample SAR dataset of 544 insider relationships as identified and described in the Methodology section of this Report.

- Changing ledgers and other records to hide their own overdraft or kiting statuses;
- Improperly crediting back overdraft fees and other service charges to themselves and others;
- Theft of equipment or information by contractors or vendors;
- Engaging in mortgage loan fraud by submitting misrepresentations of borrowers' income, employment, credit, occupancy and other requirements; submission of improper gift letters; unduly influencing appraisers to increase values; misrepresenting equity and other information to the loan committee. Loan Officers were often identified as employees in these activities.

Other

Most relationships identified in the SARs reviewed for the "other" category included former employees. Filers also reported relatives of current employees, temporary workers, loan applicants, employees of affiliates and subsidiaries, and miscellaneous vendors, among others. Some activity typologies described in these SARs included:

- Defalcation, theft or embezzlement by a former employee;
- Misuse of position of an employee, such as improper refunding of service or overdraft fees to relatives or friends, or loan application misrepresentations;
- Theft of proprietary information by a temporary staffer;
- Mysterious property disappearance attributed to the cleaning crew;
- Fraudulent or misrepresented information provided by a loan applicant;
- Improper cancellation and refund of an annuity purchased for a customer.

Broker

Broker relationships comprised four percent of the total dataset. All SARs reviewed in this category involved real estate or mortgage loan brokers engaged in mortgage loan fraud. Typical activities included submission of fraudulent information or statements, misrepresentations of occupancy or employment, or other tactics utilized in fraudulently obtaining a mortgage for which a borrower would not otherwise have qualified.

Officer

Officer relationships comprised three percent of the total dataset. In the sample reviewed, filers most frequently cited "loan officer" as the type of officer. Loan officers engaged in various commercial or mortgage loan fraud activities including misrepresenting borrower income, occupancy, employment; submission of fraudulent or altered documentation; or violating their lending limit.

Other officer relationships identified in these SARs included vice presidents, branch and department managers, and chief information officers. Filers described various types of activities in which officers engaged.

- An Executive Vice President/Chief Information Officer owned a portion of a company hired to evaluate the filer's ATM security.
- An Assistant Vice President embezzled funds by wire transferring funds from a general ledger to his own account.
- An Executive Vice President, Director and controlling shareholder misused a corporate credit card and attempted to pay the bill from general ledger funds.

Director

Director relationships were present in one percent of the total SARs in the dataset. As mentioned previously, SARs filed on directors did not report egregious activities that jeopardized the solvency of the filing institutions. Subjects identified as a Director of the institution engaged in various suspicious activities.

- A director stole and embezzled funds by deleting clearing items from the bank's system before they posted against his account;
- A director misused her position by misusing the corporate credit card;
- Filers often reported directors who owned or operated other businesses for structuring or check kiting in their business accounts;
- Directors did not disclose their own interests in loans to other entities.

Conclusion

The "employee" category far exceeded any other category of institution insider reported during the period of this study. A majority of the employee activities involved tellers and others engaging in virtually all categories of suspicious activity described in the SAR form.

The volume of annual reports of insider abuse decreased during the period of this review. While the total SARs filed on officers and directors appears small in comparison to those filed on employees, reports on those two insider groups increased slightly since 2009. The overall lower volume of SARs reporting directors and officers is consistent with government and industry experience that, for various reasons, insider abuse by directors and officers is not always detected or reported in open institutions. Nonetheless, as demonstrated by law enforcement success stories, SARs that are filed on directors and officers can be invaluable to law enforcement in organizing and preparing a successful investigation and prosecution.

Suspected Money Laundering in the Accountancy Profession – An Assessment of Depository Institution SARs to Identify Vulnerabilities and Reporting Trends

By FinCEN's Office of Regulatory Analysis

FinCEN recently undertook an assessment of depository institution Suspicious Activity Report (SAR) filings which described possible money laundering activities involving accountants, certified public accountants (CPAs) and others within the accountancy profession. Accountants are considered one type of "gatekeeper" of a financial system because persons in this profession have the ability to furnish access (knowingly or unwittingly) to the various financial transactions that might help a criminal move or conceal illicitly obtained funds.[24]

Accountants are not defined as "financial institutions" under the Bank Secrecy Act (BSA) and, thus, have no responsibility to report suspicious activities conducted by their clients, including knowledge or suspicion that the purpose of a client's

24. See various Financial Action Task Force (FATF) reports identifying money laundering typologies, including the Guidance on the Risk-Based Approach for Accountants, 17 June 2008, and Report on Money Laundering Typologies 2000-2001 (Feb. 1, 2001), available at http://www.fatf-gafi.org. Further, the U.S. Department of the Treasury, treasury authorities in other countries and the international financial community have long maintained a concern that these financial system "gatekeepers" could be used to facilitate or assist in money laundering while engaged in their professional duties for a client. As early as 1996, FATF noted the increasing number of professionals, including accountants, whose services were used to effect the placement and layering aspects of money laundering. In addition to accountants, other professions identified as gatekeepers include attorneys, trust and company service providers, notaries and other fiduciaries that assist clients with certain activities like buying and selling real estate, managing assets, or creating, operating or managing companies.

transaction is to launder funds. Although accountants maintain that such reporting could potentially encroach on the customer-client relationship, including the duty of client confidentiality, the accountancy profession has developed codes of conduct and business ethics by which their members abide, including specifying exactly how a professional can provide specific information to law enforcement without divulging confidential client information when he or she reasonably believes that certain client transactions represent an undue risk of money laundering.[25] Although accountants have no suspicious activity reporting requirements, depository institutions holding accounts for accountants may detect financial activities and transactions that the institution knows or suspects may require reporting to FinCEN.

The Federal Financial Institutions Examination Council (FFIEC) further defines accountants, as well as lawyers, investment brokers and other third parties that act as financial liaisons for their clients as "professional service providers," whose participation in illegal or questionable financial transactions may produce increased risk to financial institutions. There has been extensive international, Federal and state regulatory guidance for financial institutions to help them detect potential money laundering transactions involving professionals.[26] A professional service provider may have access to multiple accounts of multiple clients, but a financial institution may not have a direct relationship with or knowledge of the beneficial owners of those accounts. Thus, transactions involving professional service providers present third-party risks that can raise a depository institution's vulnerability to money laundering, structuring, or hiding beneficial ownership of an account holder.[27]

Furthermore, it can be difficult for a financial institution to detect money laundering activities between an accountant or CPA and his own clients because financial transactions are often conducted through multiple financial institutions

---

25. See the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) No. 54, *Illegal Acts by Clients, available at* http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00317.pdf ; and SAS No. 99, *Consideration of Fraud in a Financial Statement Audit, available at* *http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00316.pdf*. See also FinCEN's most recent relevant guidance on income tax fraud, FIN-2013-A001, "Update on Refund Fraud and Related Identity Theft," February 20, 2013 at http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-A001.pdf.
26. Federal Financial Institutions Examination Council (FFIEC,) Bank Secrecy Act/Anti-Money Laundering Examination Manual, Professional Service Providers, available online at http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.
27. Federal Financial Institutions Examination Council (FFIEC,) Bank Secrecy Act/Anti-Money Laundering Examination Manual, Professional Service Providers, available online at http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm.

in multiple countries, and often involve foreign correspondent banks. In fact, as seen in the Research and Analysis section of this article, financial institutions did not file many of the SARs examined in this study until the filers became aware of a law enforcement investigation or an indictment of the customer for improper financial activities. It does appear, however, that once financial institutions are made aware of improper financial activities, they are diligent in searching and reporting relevant transactions that passed through their financial institution. This is reinforced by the fact that, in addition to filings upon notification of law enforcement activity, some depository institutions filed SARs simply because of the presence of specific risk factors. The risk factors filers most frequently cited included transactions with high-risk jurisdictions; apparent shell company activities; multiple international transactions, including those through foreign correspondent banks; and customers involved in high-risk professions. Some of these SARs only reported that accounting itself is a high-risk profession; several even identified accountants as "gatekeepers."

Analyst's Note: The degree of control attorneys and accountants hold over their clients' finances in routine transactions can be quite different. For example, attorneys generally conduct financial transactions on their clients' behalf, and assume control over the clients' funds to do so. Lawyers must "hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property."[28] Except in unusual circumstances, client funds are pooled in a general client trust account over which the attorney acts as trustee. The accounts are referred to as "interest on lawyers trust accounts" (IOLTAs) and the interest earned on these accounts is transferred to state funds established to cover legal expenses for indigent people.

Although accountants do sometimes hold client funds in trust accounts over which they serve as trustee (which can result in some of the most egregious suspicious financial activities involving accountants), most general activities by an accountant are done in an advisory capacity, or in preparation of financial reports, which do not require the accountant or CPA to take control of client funds. Consequently, there is no legally mandated accountant-client fund pooling in the accounting industry equivalent to IOLTA accounts for attorneys.

28. See ABA Model Rules on Professional Conduct, Rule 1.15 - Safekeeping Property, available at http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_15_safekeeping_priority.html.

Significant Findings

It is difficult to categorize accountants' improper financial activities into a few major areas. In fact, the SARs reviewed in this analysis reported improper accountant involvement in every category of activity available on the SAR form, facilitated both on their own behalf as well as in assisting others. In addition some SARs alleged that accountants or CPAs embezzled money from legal trusts over which they had been legitimately appointed as fiduciary to administer the funds. Other subjects intentionally established bogus trusts for various nefarious purposes, such as to entice terminally ill or elderly persons to enter into joint investments that only benefitted the accountant trustees or other co-investors, or to sell bogus documents that promised to declare mortgages illegal and void a borrower's obligation under his mortgage.

Methodology

An analyst searched FinCEN's BSA database for SARs filed by depository institutions during calendar year 2011 where the word "accountant" or "CPA" appeared in either the subject or narrative section of the form. From a return of nearly 10,000 relevant SARs, the analyst selected a random sample of 350 SARs for in-depth analysis. The research focused on accountants or CPAs, who (1) in their capacity as professional service provider, trustee, or fiduciary; (2) manage, direct, organize, establish or conduct transactions for their clients or on their own behalf in matters involving; (3) trust accounts, shell companies, real estate transactions, incorporations, and other matters. In addition to FinCEN data, the analyst also researched domestic and some international regulatory information; supervisory and examination guidance; enforcement and compliance activities; industry guidance; news archives; state securities and insurance codes; state licensing and sanctioning records on selected individuals; criminal indictments and related press releases; and other open source records.

Research and Analysis

It is difficult to quantify a specific count of all SARs identifying suspected money laundering activities by accountants or CPAs because the results are infinite, depending on the combination of specific search terms used in the queries. In addition, all pertinent instances may not be identified by financial institutions because the institution may have limited access to financial details

of an accountant's involvement in their clients' activities, particularly when transactions and other activities are conducted through other institutions or in other jurisdictions. Some SAR filers acknowledged their inability to detect certain suspicious activities until they learned of law enforcement investigations or indictments, at which time they reviewed their customer's account activities and filed a SAR. Consequently, FinCEN reporting should be considered as one indicator of the volume of suspicious activities involving accountants or CPAs.

The purpose of FinCEN's research and analysis is to provide a qualitative overview of the most commonly observed trends and patterns in suspicious activity reporting when filers suspected accountants or CPAs were engaged or assisted in money laundering activities rather than providing a specific summary of all accountant or CPA-related SARs filed by depository institutions. Some of the criminal indictments and enforcement actions found in connection with SARs discussed in this analysis provide more descriptive scenarios than what could be gleaned from solely examining the SARs. The combination of SAR typologies and case examples may provide filers the types of possible problematic activities completed by persons involved in the accountancy profession that they may encounter at their institution.

SAR filers identified accountants or CPAs as subjects in 227 or 65 percent of the 350 SARs sampled for this study. Filers generally described the following activities in narratives of the remaining reports when the subject was not a CPA or accountant.

- Some SARs describing foreign shell company activities only noted that such companies are created in certain jurisdictions, by local teams of professionals, including attorneys, accountants and other business professionals. The filers commented that it is typical for the true owner of the shell company to use the information of the incorporating team as the address of record, without establishing an actual physical presence in the jurisdiction.
- Other SARs did not clearly describe any financial wrong doing by accountants. Reported activities in those filings included submission of fraudulent "CPA letters" and other documentation in cases of mortgage loan fraud, without making a distinction of who altered the documents. Other SARs reported that when questioning why transactions were conducted in a certain way, subjects advised that it was upon advice of their CPA.

An Overview of Correspondent Banks, Tax Havens, Shell, Shelf and Offshore Companies and Trusts

Before more fully describing FinCEN's analytic findings, it is important to consider the possible conduits used by nefarious accountants or CPAs engaged in money laundering activities. As will be discussed in the SAR examples found later in this article, filers reported money laundering, tax fraud or evasion and other financial crimes involving accountants or CPAs engaged in activities through tax havens, shell, shelf and offshore companies, and trusts, with funds frequently transacted through foreign correspondent banks. While use of these vehicles is not limited to accountants or CPAs, accountants employed such entities and mechanisms in the most costly losses and egregious activities described in the SARs.

For nearly two decades, regulators and legislators have documented money laundering risks inherent in transactions with foreign correspondent banks. Correspondent accounts in U.S. banks "provide a significant gateway for rogue foreign banks and their criminal clients to carry on money laundering and other criminal activity in the United States and to benefit from the protections afforded by the safety and soundness of the U.S. banking industry."[29]

Monetary transactions between U.S. financial institutions and tax havens, shell, shelf and offshore companies and trusts, typically flow through foreign correspondent banks. Section 312 of the USA PATRIOT Act requires U.S. financial institutions to perform due diligence and, in some cases, enhanced due diligence, with regard to correspondent accounts established or maintained for foreign financial institutions and private banking accounts established or maintained for non-U.S. persons.[30] It remains difficult for a financial institution to obtain corporate or ownership information on the legitimacy of its correspondent's customers. Consequently, a financial institution may have greater difficulty ascertaining the purpose of a transaction or source of funds, a true beneficial owner of certain trust funds, the legitimacy of transactions or the validity of a company with whom it does not have a relationship.

29. See the Minority Staff of the Permanent Subcommittee on Investigations report dated February 5, 2001 entitled "Correspondent Banking: A Gateway for Money Laundering," available at http://www.hsgac.senate.gov/subcommittees/investigations/reports?PageNum_rs=3&.

30. See 31 CFR 1010.610 - Due diligence programs for correspondent accounts for foreign financial institutions. For more information on Section 312 requirements, see http://www.fincen.gov/news_room/rp/rulings/pdf/312factsheet.pdf.

The term "shell company," as used herein, refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) in a country, and generate little to no independent economic value. A lack of transparency in the formation and operation of shell companies may be a desired characteristic for certain legitimate business activity, but it is also a vulnerability that allows these companies to disguise their ownership and purpose.[31]

A shelf company is a shell company that has been previously established and whose longevity gives the impression of legitimacy. They literally "sit on a shelf" waiting for purchase and their older incorporation date gives the appearance that they have been in business for a period of time. Shell and shelf companies are organized by teams of service providers, including lawyers and accountants, who compete for the business of new clients to establish entities in the jurisdiction of their choice, seeking corporate vehicles that will not divulge their ownership. Services include the incorporation and can also include installation of nominee directors, an address of record (usually the address of the incorporation service), assignment of tax identification numbers, and establishment of bank accounts in other countries. Web sites of multiple service providers of shell and shelf corporation services advertise the sale of complete corporate "packages" in the jurisdiction of one's choice.[32]

Some terms for these companies are used interchangeably. There is no universally-recognized definition of "offshore." An offshore financial center provides financial services by banks and other agents to non-residents. Significant funds are believed to be held in offshore financial centers in mutual funds, trusts, international business companies, or other intermediaries not associated with financial institutions. Transactions are usually initiated elsewhere, and the financial centers provide low or no taxation; moderate or light financial regulation; and, banking secrecy and anonymity. Offshore corporations, sometimes referred to as tax havens because of low or no taxes charged to foreigners, are limited liability companies registered within the offshore financial center.

---

31. For more information on the vulnerabilities posed by these companies, see FinCEN Guidance FIN-2006-G014, "Potential Money Laundering Risks Related to Shell Companies," dated November 9, 2006 found at: http://www.fincen.gov/statutes_regs/guidance/pdf/AdvisoryOnShells_FINAL.pdf.

32. See the following websites for examples of offshore company formation services in Nevis or Panama, and names of previously-incorporated corporations available in multiple jurisdictions: http://www.apintertrust.com/offshore_company/nevis_tax_haven.htm ; http://readymadeshelfcompany.com/search_by_database.php.

Analyst's Note: It should be acknowledged that the same type of service provider teams, including accountants, found in other countries, also legally exist in the United States to help U.S. and foreign citizens establish corporations here. Corporations are governed by state law in the United States, and because of lack of uniformity and lenient information collection requirements by some states at the time of incorporation, the United States has been referred to as a tax haven country. Delaware, Nevada, Oregon and Wyoming are the states most frequently said to be less restrictive in their incorporation processes. For over two decades, the United States has been working to enact or modify the lack of uniformity in state corporation processes.

Legislators have repeatedly urged states to comply with the FATF-proposed uniform standard on collection of beneficial ownership of corporations, and legislation has consistently been proposed in each new Congress seeking to curb the use of U.S. corporations for financial crime. FinCEN has also initiated outreach to the states, and issued guidance to financial institutions on potential risks associated with accounts maintained for shell companies.[33] In 2005 FinCEN conducted an analysis on the role of domestic shell companies in financial crime which was updated and released with industry guidance on November 6, 2006.[34]

A joint notice of proposed rulemaking (NPRM) issued by FinCEN and other banking and financial regulators who oversee industries with AML program requirements is currently pending. The comment period has been extended because of significant interest from multiple parties. The proposed rule will clarify and strengthen customer due diligence requirements and supervisory expectations for financial institutions to identify beneficial ownership of their accountholders.

33. See Press Release, "FinCEN Advises Financial Industry on Potential Risks of Shell Companies", November 9, 2006, available at http://www.fincen.gov/news_room/nr/html/20061109.html. See also, testimony of Jamal el-Hindi, Associate Director for Regulatory Policy and Programs Division, FinCEN, before the Senate Permanent Subcommittee on Investigations, November 14, 2006, available at http://www.fincen.gov/news_room/testimony/html/20061114.html.

34. See http://www.fincen.gov/news_room/rp/files/LLCAssessment_FINAL.pdf.

Subsequent to the original NPRM, the agencies jointly provided Guidance on Obtaining and Retaining Beneficial ownership Information.[35] This guidance specifically addressed customer due diligence procedures and foreign correspondent accounts. The U.S. Department of the Treasury/FinCEN held a series of public hearings in the summer and fall 2012. The hearings provided an opportunity for the industry, law enforcement and regulatory communities to seek further clarification on issues raised by the NPRM.

Finally, pursuant to the Foreign Account Tax Compliance Act (FATCA),[36] the United States announced agreements with France, Germany, Italy, Spain and United Kingdom to jointly develop a framework to collect and send information about offshore accounts held by Americans from their banks to the Internal Revenue Service. The Act also requires the U.S. government to provide similar ownership information. On June 21, 2012, the U.S. Department of the Treasury and the government of Japan expressed their mutual intent to pursue cooperation under FATCA. On July 26, 2012, the Department of the Treasury published a model agreement along with a joint communiqué with the five countries endorsing the agreement and calling for a speedy conclusion of bilateral agreements based on the model."[37]

BSA Research – Initial Search of 2011 SAR-DIs

FinCEN database queries using key search terms related to accountants and CPAs returned 9,631 SARs filed in CY 2011. Banks, savings institutions or credit unions filed the majority of the SARs. However, mortgage companies, mortgage service companies, credit card servicers and processors, and other financial service companies filed 250 of the 9,631 accountant or CPA-related SARs.

35. FIN-2010-G001, March 5, 2010, available at http://www.fincen.gov/statutes_regs/guidance/html/fin-2010-g001.html
36. "Hiring Incentives to Restore Employment Act of 2010," Pub.L. 222-147, Section 501(a). For additional information on FATCA see http://www.irs.gov/Businesses/Corporations/Foreign-Account-Tax-Compliance-Act-(FATCA).
37. See Press Release "Treasury Releases Model Intergovernmental Agreement for Implementing the Foreign Account Tax Compliance Act to Improve Offshore Tax Compliance and Reduce Burden, July 26, 2012, available at: http://www.treasury.gov/press-center/press-releases/Pages/tg1653.aspx.

Over 62 percent of the SARs noted Category A – BSA/Structuring/Money Laundering as the characterization of suspicious activity. Nearly 21 percent reported Category P – Mortgage Loan Fraud.[38] The third-largest activity category, at almost 13 percent, was Category S – Other. Table 1 identifies the number of filings in the most significant suspicious activity categories.

Table 1 – CY 2011 SARs: Characterization of Suspicious Activity

Suspicious Activity Description	*Total SARs*
A – BSA/Structuring/ Money Laundering	6,029
C – Check Fraud	455
D – Check Kiting	168
E – Commercial Loan Fraud	125
G – Consumer Loan Fraud	163
M – Defalcation/ Embezzlement	122
N – False Statement	408
P – Mortgage Loan Fraud	1,993
R – Wire Transfer Fraud	175
S – Other	1,237
U – Identity Theft	100

Table 2 identifies the most frequently described "Other" activities with respect to Category S.

Table 2 – Most Frequent Activities Defined in Category S – Other

Suspicious Activity Description	*Number of SARs*	*Percentage of Other SARs*
Unusual cash, check or wire activities	319	26%
Tax Fraud or Evasion	278	22%
ACH activities	50	Less than 1%
Debt elimination, advance fee scams and other aspects of mortgage loan fraud **	32	Less than 1%
Financial fraud against the elderly	32	Less than 1%
Unregistered MSBs	20	Less than 1%

****These SARs did not specifically include Category P - Mortgage Loan Fraud.**

38. The combination of mortgage, consumer and commercial loan fraud SARs is 2,313, making loan fraud activities an even higher 24 percent of all activities in which accountants or CPAs engaged in the 2011 SARs.

Expanded Research

In the 350-SAR sample, filers most frequently cited the suspicious activity characterization as Category A – BSA/Structuring/Money Laundering (52 percent). Twenty-six percent reported Category S – Other. The third largest activity category, at almost 19 percent, was Category P – Mortgage Loan Fraud. Table 3 identifies total filings in the most significant activity categories.

Table 3 – Characterization of Suspicious Activity (350-SAR Sample)

Suspicious Activity Category	*Total SARs*
A – BSA/Structuring/ Money Laundering	184
C – Check Fraud	14
D – Check Kiting	5
E – Commercial Loan Fraud	7
G – Consumer Loan Fraud	9
M – Defalcation/ Embezzlement	8
N – False Statement	35
P – Mortgage Loan Fraud	66
R – Wire Transfer Fraud	9
S – Other	92
U – Identity Theft	8

As shown in Table 3, 92 SARs reported Category S – Other. Many activities were identified less than five times. The activity described by filers in the sample set that marked "Other" generally mimicked that reported in the full dataset.

Note that the SARs sampled by the analyst for full review mimic the same top three activity categories as the statistical review of all 9,631 SARs filed in 2011 which mentioned accountants or CPAs in either the occupation or the narrative field. Table 4 identifies the percentages of the top three activity categories in the original search of 9,631 compared to the 350 SARs which were reviewed in their entirety for this analysis.

Table 4 – Top Three Activity Categories – A Comparison

Suspicious Activity Category	*Original Statistical Search Only – All Relevant SARs filed in 2011 (9,631 SARs)*	*Percentage of Total*	*SARs with Full Review and Analysis (350 SARs)*	*Percentage of Total*
A – BSA/Structuring/ Money Laundering	6,029	63%	184	53%
S – Other	1,237	13%	92	26%
P – Mortgage Loan Fraud	1,993	21%	66	19%

Significant Money Laundering Trends and Patterns by Accountants or CPAs

Some SARs in this analysis reported accountants or CPAs who committed money laundering transactions for their own benefit, such as simple structuring or tax evasion. Other SARs, as well as indictments and other legal documents, also show that accountants or CPAs facilitated money laundering on behalf of others by helping to hide aspects of transactions through various schemes. Accountants or CPAs may sometimes also act as directors, trustees or partners in these transactions. The remainder of this article provides trends associated with specific activities filers described in SARs and information gleaned from a review of criminal indictments and other open source documents.

BSA/Structuring/Money Laundering

- In addition to structuring and money laundering, this category identified a wide variety of activities including wire transfers to and from foreign countries, including high-risk countries and professions; inconsistent account activity; multiple transfers between accounts; transaction purposes that could not be verified; shell company activities; and improper trust activities.
- Some non-accountant subjects admitted to structuring in order to deceive their accountant from full facts about a transaction or having been done on the advice of their accountant.

Tax Fraud or Evasion

- Some accountants improperly received electronic deposits of income tax refunds that were due to other persons. Filers sometimes identified this activity as ACH fraud. In other cases, accountants submitted tax returns for deceased persons and deposited the tax refund to their own account.
- Individuals admitted to filers they had committed tax fraud by withholding information from their accountant. One subject said he dealt in cash rather than submitting records to his accountant so the accountant would not include the amount as part of his income on Federal and state tax filings.
- A bank filed multiple SARs after law enforcement arrested a group of individuals, several of whom were current or former CPAs, who conducted seminars where they sold "tax-exempt trusts" for $500-$1,000. Two accountants in the group were sentenced to up to three years' incarceration,

respectively, for multiple counts of conspiracy, mail fraud, and failure to file tax returns. The leader, sentenced to over 10 years in prison, was said to have profited by over $8 million during a 10-year period of perpetuating the scam.

- A securities broker and a branch of its subsidiary bank filed SARs on an individual in the entertainment field who had established two irrevocable trusts at the bank. When this customer subsequently applied for a line of credit, the filer discovered that the customer's company was actually an offshore trust. The individual's CPA and an offshore corporation formation company served as co-trustees. The irrevocable trust accounts had received wires totaling nearly $1 million from the offshore address, via an account in a Swiss financial institution. The subject informed the filer that his CPA had advised him to establish the trust in order to preserve his assets in the event he was sued as a member of the highly litigious movie industry. The SARs did not provide a specific type of suspicious activity associated with the trust accounts.

Mortgage Loan Fraud

- Some accountant borrowers committed mortgage loan fraud on their own behalf by providing false financial or occupancy information with their loan application.
- In order to appear better qualified for a loan, some non-accountant borrowers committed mortgage fraud by altering documents that had been prepared by their accountant.
- Numerous SARs reported altered or falsified "CPA letters," a requirement for approval of some mortgage loans. The filers generally did not explain whether the CPA, the borrower, or someone else, altered the documents.
- Mortgage loan fraud by accountants or CPAs also involved loan modification, debt elimination or short sale fraud schemes in cases of pending foreclosure.
- A credit union filed multiple SARs to report a local accountant/owner of a tax preparation business suspected of structuring cash deposits and withdrawals. According to the indictment, the accountant helped clients of complicit realtors to obtain mortgage loans by creating fraudulent tax letters stating the borrowers had self-employment income and owned their own businesses. He and his employees also prepared fraudulent tax returns with the knowledge that they were not intended to be filed with IRS. The accountant's fraudulent tax letters resulted in losses of more than $2 million in fraudulent loans to clients who had no ability to repay the loans. The individual pled guilty to conspiring to commit bank fraud and was sentenced to 2 years in prison.

Defalcation/Embezzlement/Theft

- A SAR filer reported its accountant customer for money laundering, check fraud, credit card fraud, and embezzlement. The customer, employed in a CPA firm, obtained access to the business checking accounts of one of the firm's clients. The accountant forged several of the client's checks, payable to the filer, and used the funds to pay a personal credit card. The filer notified law enforcement, but the outcome of an investigation is unknown.
- A SAR described activities by the filer's CPA customer, who had been arrested on larceny and money laundering charges. The CPA allegedly embezzled and mishandled funds of over $500,000 due to the subject's access to multiple trust accounts. The subject also served as Chairman of the Board of another local bank.
- A bank filed a SAR against its accountant employee upon discovering that the accountant embezzled funds by making transfers from the bank's general ledger account into a personal account. No further law enforcement information was located.

Correspondent Accounts

Transfers through foreign correspondent banks enable the laundering of illicit funds through the U.S. financial system and can hide the source of the funds, purpose of the transactions, or the beneficial ownership of businesses.

- A large bank filed SARs on multiple international companies for suspicious activities conducted through its correspondent bank customers. Locations for some of the parties to the suspicious transactions included Cyprus, the United Kingdom and Gibraltar. Locations for other parties could not be identified. Individuals sent wires by order of or for the benefit of possible shell entities, some of whom appeared to be connected to Internet gambling. The bank suspected that the entities did not really exist, although one of the involved banks reassured the filer that it is common for companies registered in Cyprus to provide the address of its lawyers or accountants as its business address.
- A large bank filed several SARs on its customer, a United Arab Emirates (UAE) trading company. The customer transacted with numerous businesses in multiple countries via correspondent banks. The filer stated the companies are apparent shells using addresses in offshore jurisdictions about which no information could be found. The nature, purpose and source of the funds

for transactions could not be identified. The customer was also a client of a renowned CPA firm in Dubai. The SAR reported movement of funds between high risk jurisdictions.

- A filer described suspicious activities by a customer, a Venezuelan lawyer. Because of currency controls in Venezuela during the past decade, the subject assisted other Venezuelans in establishing foreign companies through which funds could be hidden outside of Venezuela. The subject worked with an accountant in Curacao who established the companies and opened bank accounts in the United States and other foreign countries. Using correspondent bank accounts, transactions flowed into the subject's account with the filer on behalf of different individuals and companies.

Shell Company Activities

The majority of SARs involving shell company activities described multiple transfers through shell companies located in multiple jurisdictions, sometimes through the use of correspondent banks.

- A SAR filed on a real estate company owned by a husband and wife also included their minor child and their CPA as subjects, and described shell account and tax evasion activities. The filer reported that the minor child had attempted to open a business account for a limited liability company (LLC) to be established to purchase investment real estate. The filer's BSA officer suspected that an LLC headed by the minor could be a shell company created to protect the true beneficial owners who were controlling the finances (such as the parents avoiding tax implications by not being directly linked to the LLC). The SAR provided no information about the specific activities of the CPA.
- A bank filed SARs on multiple companies with no known physical locations. Other subjects had addresses in Venezuela, the United Kingdom and Tortola. The bank identified one subject as a United Kingdom chartered accounting firm whose customer was a shell company chartered in the British Virgin Islands whose business was identified as "private investments." The principals of the company also owned a jewelry store in a country in South America. Activities involved wires to and from offshore companies, sometimes through offshore banks. The filer could not identify the purpose of the transactions and provided no indication of subsequent law enforcement activity.

- A bank filed a SAR on multiple entities in locations that included New Zealand, Latvia, and the United Kingdom. The subjects also owned companies in Switzerland, Germany, China, and other countries. The SAR described nesting[39] and shell-like wire activities through correspondent accounts. One of the ordering entities was a "chartered accountant."

- Banks filed multiple SARs on executives of a U.S. manufacturing company for creating multiple shell companies through which they kited funds to give the appearance of more wealth than the company actually had. The individuals used this appearance of wealth to defraud institutions into providing loans to the company, the proceeds of which were diverted to its principals, including its accountant. The company's CPA pleaded guilty to charges of conspiracy and wire fraud in assisting in the looting of the firm, ultimately diverting $1 billion to a shell company. A judge sentenced the CPA to three years' incarceration and ordered the defendant to pay restitution of over $20 million.

- Some SARs also reported, in addition to foreign jurisdictions, groups of professionals in the United States, including accountants, who established domestic shell companies for foreign entities. Filers commonly identified Washington, Delaware, New York, Arkansas and Oregon as states in which Russian or Eastern European foreign owned companies incorporated. Filers also suggested that Nevada and Wyoming were receptive to foreign entities registering shell companies within their jurisdictions. The entities then gained access to the U.S. financial system by opening accounts at local banks.

Shell companies and securities fraud

Shell companies are also used to "bid up" prices of worthless stocks, called "pump and dump schemes," in which scammers flood media and news sites about the latest "hot" stock. People are encouraged to buy the stock, which they do. This creates a high demand and "pumps up" the price. The scammer then sells his shares at the peak price and the stock plummets and the investors lose their money.[40]

- Following several law enforcement investigations, banks filed multiple SARs on a CPA and his attorney partner for operating several pump and dump schemes over the last decade. An SEC Civil Complaint charged the accountant

39. "Nesting" refers to the use of a foreign bank's correspondent account with a U.S. bank by another foreign bank to gain access to the U.S. banking system. See "The Role of Domestic Shell Companies in Financial Crime and Money Laundering: Limited Liability Companies, FinCEN, November 2006.

40. SEC "Pump & Dump Cons – Tips for Avoiding Stock Scams on the Internet" available at http://www.sec.gov/investor/pubs/pump.htm.

and attorney with a scheme to create and sell multiple Nevada and Delaware shell companies for over $7 million. All companies had been set up with nominee directors and managers, and some registered with the SEC. The two subjects were subsequently indicted on tax evasion charges from the profits they earned in the sale of the shell companies. The CPA pleaded guilty to tax evasion charges and faced a maximum sentence of 5 years in prison and a maximum fine of $250,000. After cooperating with the prosecution, the CPA was sentenced to a few months in prison, a few months of community confinement and several years of supervised release. He was also ordered to pay a $2,000 fine and almost $400,000 in restitution for tax evasion.

- A bank filed a SAR following media reports of a local lawyer found guilty for stealing millions of dollars from investors through a pump and dump scheme. The scheme involved shares of stock illegally sold for a company in another state. A local CPA was named as an unindicted co-conspirator for selling the stock into the public market.

Improper trust activities

BSA filings and indictments show that some of the most egregious and expensive financial crimes involving accountants or CPAs occur when they steal from clients or investors to whom they owe a fiduciary duty based on access to or control of the clients' funds held in trust.

- **Investments with Terminally-Ill Persons**

  - Several SARs described investments for terminally-ill persons. Subjects included attorneys, accountants, CPAs, end-of-life care companies, and investors. The subjects coerced terminally ill or elderly persons to agree to participate in transactions in which the dying person received cash payments or other concessions. Instead, subjects used the individuals' personal information to establish joint investment vehicles with unknown conspirator investors.

- **Theft and embezzlement from accounts over which the CPA serves as Trustee**

  - Depository institutions filed multiple SARs on a CPA who owned a forensic accounting firm, and was appointed receiver and/or trustee for various Federal and State proceedings over the past decade. The CPA had been an expert witness for the government in multiple liquidating receiverships. A Federal Grand Jury subsequently indicted the subject.

The CPA sometimes worked with a close relative, who was indicted for mail fraud. Court records showed that for nearly a decade, the CPA, while living a lavish lifestyle, wrote unauthorized checks to himself or his company from the receiverships or accounts over which he served as trustee. The court stated the CPA used some of the money from unrelated fiduciary accounts under his control to repay shortfalls in the depleted fiduciary accounts by moving funds, in a Ponzi-like fashion, into the depleted accounts. An indictment charged that the CPA issued over 150 unauthorized checks and misappropriated at least $6 million from numerous cases to which he had been appointed fiduciary. The CPA pled guilty, and was sentenced to eight years in prison, with an additional 21 months in house arrest.

- Banks filed multiple SARs against a CPA and investment advisor, who had many high profile and high net worth clients, including socialites and well known entertainment and business figures. The CPA managed his clients' finances, paid their bills, provided tax advice and made investments on their behalf. An SEC civil complaint charged that he and his company misappropriated over $7 million from client accounts over which he had access. The complaint noted violation of the Investment Advisers Act of 1940. The SEC subsequently charged the CPA's attorney with aiding and abetting the CPA's fraud by using his own attorney trust account to hide the scheme. The complaint stated that millions of dollars belonging to the CPA's clients flowed through the attorney's accounts. To perpetuate the scheme, the CPA stole money and transferred funds without authorization from the client funds into the attorney trust accounts. The attorney subsequently transferred the stolen funds to the CPA and entities controlled by him. The CPA pled guilty to securities fraud, wire fraud and money laundering. According to legal documents, the total loss associated with his fraud was between $20 million and $50 million and he admitted to stealing over $30 million in his guilty plea. He was sentenced to approximately 7 ½ years in prison.

- One bank filed several SARs to report an accountant and auditor's activities involving defalcation/embezzlement, larceny, BSA/Structuring/Money Laundering and other actions regarding multiple businesses and trusts of various individuals of which he was a signer or associated with. The subject also served as chairman of another local bank, and institutions had filed previous SARs on him for kiting funds between the two financial institutions. He was arrested and charged with multiple offenses.

Elder Fraud

Multiple SARs reported situations in which an accountant or CPA acted as trustee on behalf of an elderly individual and diverted trust assets to themselves. The following are several patterns detected from the activities described by filers.

- A CPA prepared tax returns for an elderly individual. Using this individual's personal information, the CPA established a trust whose purpose was to purchase investment rental properties. He then fraudulently established himself as trustee. In this capacity, the subject obtained a loan in a significant dollar amount for investment purchases. The CPA's fraudulently prepared tax returns inflated his elderly client's income and assets in order to create the appearance that the trust qualified for the loan. The SAR filer further reported that a relative of the CPA, a realtor, received a commission from one of the purchases.
- Another SAR described a CPA who opened an account as trustee for a family life insurance trust account, the owner of which was an elderly female. The subject deposited forged checks payable to the trust and subsequently wrote a check against the trust payable to him. He also made online transfers to his account at another bank. There is no indication in the SAR that the subject was related to the elderly victim or her family.

Foreign Corrupt Practices Act/Politically Exposed Persons

- A bank filed multiple SARs on a South American accountant, his shell company located in his country, and an attorney from another country, who was employed as a staff member of the cabinet of a South American country, and considered by the filer to be a politically exposed person (PEP.) The filer made a real estate loan for the purchase of a condominium in the United States in the name of a foreign company, which was guaranteed by its president, the South American accountant, who was the sole signer on all of the loan documents and sole shareholder of the company.

  The bank filed the SARs following media reports that the accountant had been charged with laundering drug trafficking proceeds in South America and had also been identified as a participant in illegal gold and weapons activities. He was described as an expert in forming offshore shell companies used to launder funds obtained through his illegal financial activities. The filer determined that the accountant might have been a straw buyer for the foreign attorney.

- Subsequent to hearings held by the United States Senate Permanent Subcommittee on Investigations entitled "Keeping Foreign Corruption Out of the United States: Four Case Histories," a bank undertook an investigation of transactions by its account holder business customer, later determined to be a U.S. shell company established to manage certain expenses for the relative of a president of an African country. A CPA in the United States served as one of two persons with signatory authority on the account. The account review revealed millions of dollars in incoming wires from businesses abroad, followed by outgoing expenses. The filer determined that the incoming funds represented diversion of government funds into a U.S. shell account created for that purpose, consistent with foreign corruption investigated by the Senate subcommittee.

Summary

The purpose of this analysis is to identify trends, patterns or possible "red flag" indicators obtained from SARs reporting suspected money laundering activities by accountants or CPAs. As shown in the report, accountants and CPAs may be involved in all aspects of money laundering, facilitated both on their own behalf as well as in assisting others. They may knowingly participate in suspected money laundering activities, or unwittingly be used to give an appearance of legitimacy to a transaction. SARs reviewed in this analysis reported all available suspicious activity characterizations identified on the legacy form in Item 35. Furthermore, the reported activities are similar to at least nine of the IRS' "Dirty Dozen Tax Scams for 2012."[41]

Financial institutions have challenges in detecting some suspicious activities and transactions. Those activities include: (1) instances in which the financial institution does not have a direct relationship with the accountant or CPA, such as in correspondent banking transactions, (2) shell company activities, both domestic and international, and (3) improper trust activities, both domestic and international.

41. Available at http://www.irs.gov/uac/IRS-Releases-the-Dirty-Dozen-Tax-Scams-for-2012.

The 314(b) Program A Decade of Information Sharing: Stronger Than Ever

By FinCEN's Office of Special Programs Development

In the wake of the September 11 terrorist attacks, the USA PATRIOT Act was passed by Congress and signed into law on October 26, 2001. Among the many tools provided to law enforcement and the business community to combat money laundering and terrorist financing under the USA PATRIOT Act, Section 314(b) is unique. Under Section 314(b), a financial institution or an association of a financial institution may voluntarily share information with other financial institutions "for purposes of identifying and, where appropriate, reporting activities that the financial institution or association suspects may involve possible terrorist activity or money laundering." Having appropriately registered with FinCEN, institutions and associations may share information under the protection of "safe harbor" from liability to the "full extent provided in subsection 314(b) of Public Law 107-56 [the USA PATRIOT Act]."[43]

The following study examines the use of the 314(b) mechanism by financial institutions through the prism of SARs filed by those institutions since the inception of the program. Trends in suspicious activities gleaned from recent SAR filings are revealed. The benefits of the 314(b) program, both to participants and to law enforcement, are also highlighted.

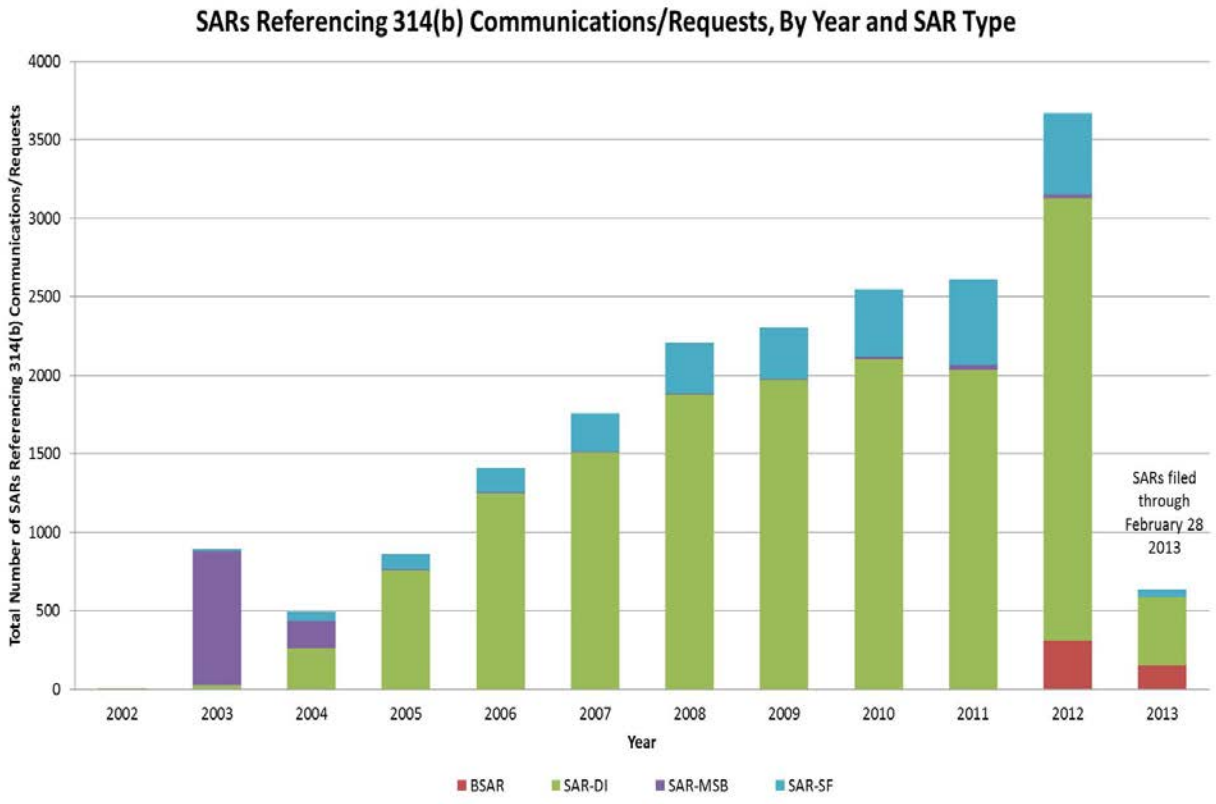
More SAR filings, Greater Variety of Participants

Over the last decade, information sharing via "314(b) communications" or "314(b) requests" has wrought substantial benefits for law enforcement and industry alike. FinCEN has received over 19,500 SARs explicitly referencing the sharing or attempted sharing of information through the 314(b) process since 2002.[44] It should be noted here that an undetermined number of SARs may also have been filed as a result of the filing institution's involvement in a 314(b) communication, even though there is no specific mention of 314(b) in the SAR narratives. As shown in the following chart, from a total of two SARs referencing 314(b) filed by financial institutions in 2002, the number of 314(b) SARs has rapidly *and* steadily grown, to 3,671 314(b) SARs filed in 2012:

42. *See* 31 C.F.R. § 1010.540.

43. 31 C.F.R. § 1010.540(b)(5)(i).

44. Over 19,500 SARs received from 2002 through February 2013.



Through the first two months of 2013, 643 SARs have been filed referencing the 314(b) program, matching 2012's pace. The steadily increasing use of the new BSAR form (also referred to as the "FinCEN SAR") should also be noted.

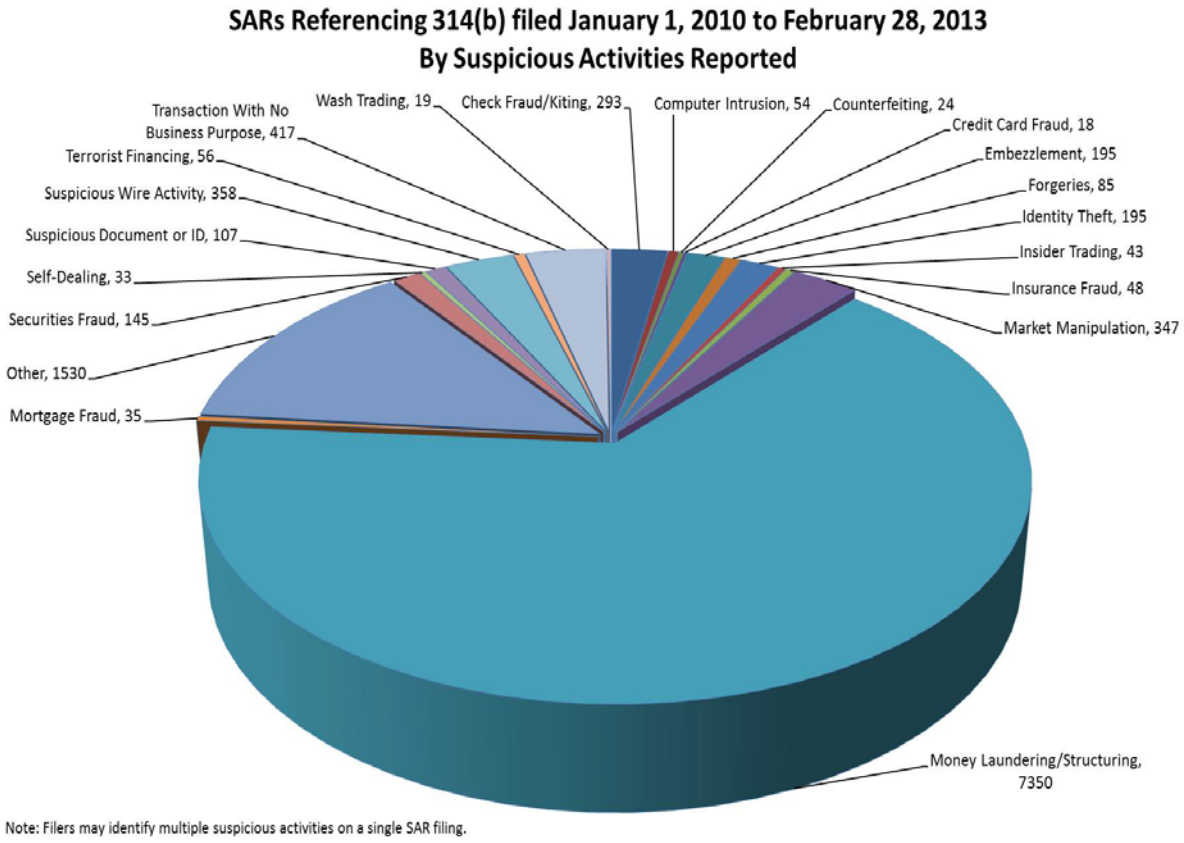
Although the majority of 314(b) SARs have been and continue to be filed by banks, we also see the increasing presence of other sectors of the financial industry among recent SAR filers who participate in the 314(b) process—including money services businesses, insurance companies, and securities firms. We can see from the data that SAR-SFs filed by securities firms and broker-dealers have increased steadily in absolute numbers, and similarly have increased overall as a proportion of the number of SARs referencing 314(b) communications.

The significance of this trend should not be overlooked. As more industries are subject to the requirements of the Bank Secrecy Act and become aware of the 314(b) process, the number of participants has increased. Concurrently, SAR filings referencing use of 314(b) communications has grown, due in part to an increasing number of participants, as well as to the comprehensive information set available to 314(b) participants, which can be used to more effectively identify and potentially report suspicious activities and entities. Moreover, the synergy developed between

314(b) participants from different sectors of the financial system—for example, between an online broker-dealer and a bank—creates opportunities for cross industry sector information sharing that may translate into determinations by one or both 314(b) participants that SARs should be filed. No SARs may have been filed in the absence of the 314(b) communication.

Recent Trends in Suspicious Activity as Conveyed by 314(b) related SARs

This study also took a look at a more recent batch of 314(b) SARs filed (since 2010) to discern overall patterns and trends on the types of filers who have been using the process and the types of suspicious activities they have been identifying. An overview of the types of activities being identified is summarized in the chart below:



Note: Filers may identify multiple suspicious activities on a single SAR filing.

Newer Sectors of the Financial System Are Increasing Their Participation

As mentioned above, the SARs reveal the use of the 314(b) mechanism to facilitate sharing of information across financial institutions from different slices of the financial sector. Banks continue to contact other banks using the 314(b) process, but they have been joined by broker-dealers, securities clearing firms, money services businesses, and insurance companies.

It is evident that the population of 314(b) participants who file SARs referencing the 314(b) mechanism has become more diverse. Relatively new sectors, such as online broker-dealers and insurance companies, have been filing a significant number of SARs referencing 314(b). Although entities from these sectors have been filing some SARs for years, the overall increasing number of SARs filed, as well the greater variety of filers from these sectors, also implies that the use of the 314(b) process is becoming more common.

Information available to the financial institutions via 314(b) allows the financial institutions the opportunity to more effectively investigate potential suspects and their activities. Financial institutions that participate in the process, as well as law enforcement that see SARs filed by one or both institutions, can obtain a more comprehensive picture of the subject's accounts, funding mechanisms, and activities. With the enhanced information available to institutions that participate in the 314(b) process, institutions can make better informed decisions and strengthen their compliance efforts.

For example, in one recent SAR, an online broker-dealer observed suspicious behavior by one of its clients. Having no face-to-face interaction with this client and unaware of its personal business, the online broker-dealer utilized a 314(b) request to communicate with the client's banks to try to further determine the relationship between the client and the recipients of related wire transfers conducted by the client. Through the 314(b) information sharing process with the banks, the broker-dealer determined that there was no relationship between the client and the recipients of the large sums of wire transfers. Without the 314(b) communication, the online broker-dealer would not have had further reason to suspect fraudulent activity.

Conversely, a 314(b) request may also explain the wire transfer activity conducted by a customer, assuaging fears of potential wrongdoing. Essentially, through the 314(b) mechanism, participant financial institutions, often from different industry sectors, can inform one another about the typical activities in which they observe mutual subjects of concern engaging, thereby assisting in verifying whether or not the subjects' activities are actually suspicious. Through the 314(b) process,

important elements of a financial institution's anti-money laundering program, including its due diligence and suspicious activity monitoring and reporting efforts, can be augmented with the infusion of additional information, often stemming from financial institutions involved in other diverse sectors.

314(b) is Being Used to Validate Subject Information and Activities

Our study has also revealed that financial institutions appear to be using the 314(b) mechanism to verify information, such as a suspect's identity, trading patterns, and the validity of checks or other documents issued by other financial institutions.

For example, in a recent SAR, a financial services company described receiving a suspicious check from a client issued by another financial institution. The company placed a 314(b) request with the issuing financial institution. Through the response, the financial services company was informed that the routing number on the check was old and did not belong to the suspect trying to deposit the funds into their account.

In another instance, a SAR filed by a U.S. broker-dealer reported their being approached by subjects from an Asian country who attempted to open an account with one of the broker-dealer's agents, claiming that they represented a foreign national who possessed an account worth $50 billion with the Hong Kong branch of a large bank. The subjects wanted to invest $100 million through the broker-dealer. The broker-dealer filed a 314(b) request with the bank to verify the legitimacy of the documentation provided by the subjects. Through the 314(b) communications process, the bank informed the broker-dealer that the documents were, in fact, fraudulent. Moreover, the bank informed the broker-dealer that one of the subjects had apparently approached the bank's New York branch, claiming to be a customer of the Hong Kong branch. The broker-dealer continued to monitor the activity of the subjects, never actually opened an account with the subjects, and filed a SAR including all of the aforementioned details.

Similarly, two SARs highlighted the use of the 314(b) process between two broker-dealers who together were able to determine that a suspect, who had been a financial advisor with one of the broker-dealers before being terminated, was impersonating his clients and engaging in forgery and market manipulation. The allegedly impersonated individuals were originally clients, via the subject, of one of the broker-dealers and had recently switched their accounts to the other firm. The new clients all bought stock with a "micro-cap" firm which was partially owned by the suspect. Since the new broker-dealer was not familiar with these clients, and was suspicious of the activities, the broker-dealer initiated a 314(b) request with the former broker-dealer,

which initiated its own investigation. As a result, the new broker-dealer confirmed its suspicions of forgery, impersonation, and market manipulation, terminating its relationship with the suspect and filing a SAR that included details provided by the former broker-dealer through the 314(b) process. Meanwhile, the former broker-dealer investigated further, initiated a 314(b) request with a *third* broker-dealer, determined to monitor all accounts with holdings in the suspect's micro-cap firm, restricted any remaining accounts related to the suspect, and filed a SAR.

Money Laundering and Structuring: The Prevalent Suspicious Activity Type

The vast majority of SARs filed referencing 314(b) inquiries involve potential money laundering and/or structuring as the primary suspicious activity type. Although a growing number of 314(b) SARs are being filed involving other activities, the bulk of 314(b) SAR filings involve potential money laundering and/or structuring. The 314(b) process is particularly well-suited to enable financial institutions to obtain information regarding potential money laundering and/or structuring. For example, a large national bank may notice an individual customer making cash deposits several days in a row, each just under the reporting threshold for CTRs. Through the 314(b) mechanism, the bank can contact the customer's other bank(s) to determine the source of funds, and to discover if the suspect is engaging in similar behavior with other financial institutions. In another reflective example, a broker-dealer may receive deposits from investors in the form of three separate cashier's checks, each purchased at a bank with $9,000 in cash—again, just under the CTR reporting threshold. Through a 314(b) request, the broker-dealer can communicate with the bank that issued the cashier's checks to see how the checks were obtained.

The 314(b) SARs also reveal that potential money laundering and/or structuring frequently occurs in conjunction with other illegal activity such as forgery, check fraud, securities fraud, suspicious wire activity, or other transactions without apparent economic purpose. For instance, in one recently filed SAR, an online broker-dealer noted a suspicious pattern of ACH deposits followed immediately by ATM withdrawals conducted by two separate and apparently organized groups of clients. The transactions appeared to lack any economic purpose. Both groups involved an ATM operator. The 314(b) process was used by the broker-dealer to communicate with several of the clients' banks, and as a result, the broker-dealer was able to establish that some of the ACH deposits with which the clients funded their broker-dealer accounts were funded with cash, the ultimate source of which is unknown. The pattern of activity suggested that the clients in each group worked in concert to potentially defraud the online broker-dealer through excessive ATM fees

rebated back by the broker-dealer to the ATM operator. The broker-dealer was also able to further determine from the information sharing that the suspect clients were engaging in this activity across the country.

Terrorist Financing

The study has also observed that for nearly every year since the program's inception, the use or attempted use of the 314(b) mechanism to exchange information on subjects and activities has resulted in the filing of SARs involving potential terrorist financing activity. Overall, there are very few 314(b) SARs involving potential terrorist financing, less than 200 SARs since 2003. However, they are consistently filed every year by financial institutions, and are, by their very nature, particularly significant, garnering considerable attention from law enforcement. The 314(b) communication process in these situations can be vital to provide the most comprehensive picture of these particularly sensitive subjects and their activities to law enforcement. Recent 314(b) SAR filings in this area, for example, have involved individuals and entities that conducted activities which involved parties residing in countries that have been identified as state sponsors of terrorism, and/or have been linked with known terrorist organizations as well as organized crime.

Insurance Fraud and Scams

Insurance companies have been filing SARs referencing the use of the 314(b) process since 2007. The study has observed a marked increase, over the past few years, in the number of 314(b) SARs filed by the insurance industry. The 314(b) process allows insurance companies to contact banks, other insurance companies, and other financial institutions to help identify the true source of funds when a policy is purchased or financed in a peculiar fashion. For example, a recent SAR revealed an individual paying for a life insurance premium through a wire transfer. The insurance company contacted the sending bank to find out where the wire was sent from and attempted to isolate the source of funds. The information provided by the bank revealed that the wire transfer emanated from other individuals who had no documented relationship to the policy holder.

In another recent example, a SAR described the 314(b) communication made by one insurance company to another insurance company regarding the contacted insurance company's agent. The originating firm had obtained financial information from a bank using 314(b) that identified the suspicious activity of the contacted insurance company's agent, which included the sale of a Stranger-Owned Life Insurance, or "STOLI," policy to an elderly couple funded with suspicious funds transfers. The originating firm alerted the contacted firm to the agent's activities,

and provided the contacted firm with the information they had collected. The contacted firm initiated an investigation of their agent as a result, including, in turn, the use of the 314(b) process to obtain more information from the bank contacted by the originating firm. As a result, the contacted firm filed a SAR on its agent.

314(b) Participation Encourages "Heads up" Exchange and Cooperation among Financial Institutions

As we have illustrated in several examples, a central benefit of participating in the 314(b) process is that a financial institution that is aware of suspicious activity can employ 314(b) communications not only to gather information, but to alert other financial institutions to suspicious customers and their activities. For example, a recent SAR described a broker-dealer contacting a bank via the 314(b) process to inform the bank that an elderly mutual client may have been the victim of an advanced fee fraud, styled as an e-mail claiming that the client had won a lottery, resulting in the activity being brought to the attention of the bank's investigative realm.

In another example, personnel at one bank noticed suspicious wire activity involving a customer consisting of a large incoming wire transfer in which the sender held a line of credit at another bank. Personnel at the first bank used the 314(b) process to contact the second bank, which was also in the process of investigating the outgoing wire transfer, the source of funds of which was apparently accessed without authorization. By expeditious cooperation on the part of the two banks' 314(b) personnel, as well as contact with the customer, the banks were able to put the pieces of the puzzle together, and with the customer's consent, the first bank was able to return the funds transferred to the second bank, and filed a SAR on the attendant suspicious activity.

Interestingly, the study also observed that many SARs referencing 314(b) communications were filed by the *contacted* financial institution, and not just the requesting financial institution. Information shared through 314(b) communications often results in a "heads up" to the receiving financial institution to more closely examine certain customers and accounts that might not otherwise have risen to this level of enhanced scrutiny.

For example, one SAR described the use of the 314(b) mechanism by a financial company to communicate to a bank that one of their mutual clients was under investigation, and that a federal law enforcement agency had obtained a seizure warrant on one of the suspect's accounts. The illicit funds were allegedly obtained from narcotics trafficking, and were commingled with legitimate funds from the suspect's business. Through the 314(b) request, the bank became aware of its client's

potentially illicit behavior and proceeded to monitor their accounts. With financial institutions facing the challenge of a proliferation of clients and accounts, this type of alert shared via the 314(b) process is vital.

As noted in another SAR, a financial institution used the 314(b) mechanism to warn another financial institution of a client's attempt to forge documents and withdraw funds that did not belong to the client. It was further discovered through the aforementioned 314(b) communication that the suspect had wired large amounts of money to various banks for relatives in high-risk countries and engaged in forging letterheads sent to other banks to approve the large transfer of illicit funds. This is an excellent example of how the 314(b) information sharing process can be proactively used to alert other financial institutions to potential illicit behavior and related pending investigations, and to uncover previously unknown suspicious activities.

Identity Theft/Computer Intrusion

As mentioned in previous examples, the study also reveals 314(b) SAR related trends in identify theft and computer intrusion reporting. With the burgeoning utilization of online technologies and the Internet for both communication and commerce in the 21st century, a rise in identity theft and computer intrusion as suspicious activity types in unsurprising. A typical example among recent 314(b) SAR filings found a securities broker describing the hacking of a client's e-mail. The hacker impersonated the client and attempted to wire all funds out of the client's account into a third-party account at a bank. The hacker did not succeed due to internal controls procedures at the broker. The broker used the 314(b) information sharing process to alert the bank about the hacker's activities.

Broker-Dealers and the Emergence of eCommerce

As addressed earlier, the study also reveals a steady rise, over recent years, in the number of SARs filed by members of the securities and futures sectors of the financial industry. Information sharing under 314(b) has become commonplace among a number of large and small broker-dealers, mutual funds, securities firms, and clearing firms, to name a few. In particular, for entities such as online broker-dealers that conduct business exclusively online, the ability to obtain additional information about their customers from other financial institutions can be invaluable for maintaining the integrity of their due diligence and transaction monitoring efforts. The number of SAR filings referencing the use of the 314(b) mechanism by online broker-dealers has increased in recent years. A number of the SARs have noted the use of online investors to transfer illicit funds. Communicating via the

314(b) mechanism enables banks to contact online broker-dealers, and vice versa, to further investigate and hash-out the overall patterns of a subject's potentially fraudulent behavior.

For example, in a recent SAR, an online broker-dealer observed the movement of suspicious funds into and out of a client's account and initiated a 314(b) communication with the bank that was the source of the suspicious deposits. In response to the 314(b) request, the bank revealed that the suspicious funds originated via ACH deposit from a corporate account maintained at the bank, and that the corporate account was funded with large cash deposits as well as large wire transfers from yet another corporate account. It is possible that the corporate accounts were controlled by the client. Funds deposited in the client's broker-dealer account were sent via wire transfer to a bank account in Indonesia, ostensibly to purchase merchandise. Essentially, this SAR illustrates how 314(b) inquiries allowed financial institutions across the industry spectrum to share information to piece together an overall complex cross-border money trail, providing evidence of activity consistent with structuring and money laundering.

Insider Trading

Another recently observed trend reveals how 314(b) communication can allow financial institutions to investigate potential insider trading. Several recent SARs showed how financial institutions used the 314(b) process to investigate suspicions of insider trading.

One SAR revealed that a securities firm suspected a client of insider trading, due to highly unusual stock purchase and trading patterns being exhibited by the client within a broker-dealer company. Through a 314(b) information exchange, the broker-dealer informed the securities firm that the individual was unemployed and had bought substantial stock because he heard about the company "through a friend." However, the subject did not reveal the exact reasoning behind the large purchase of stock shares, and as a result, the requesting securities firm filed a SAR.

In another example, an online broker-dealer identified a client who was a partner at a securities law firm and whose trading activity exhibited signs of potential insider trading and market manipulation. The broker-dealer received an ACH deposit into the client's account from a third-party's bank. One week later, the client withdrew the exact same amount from his broker-dealer account and then deposited it into the same bank account from which he had received the initial ACH deposit. Through

the 314(b) information sharing process, the broker-dealer was able to obtain account and source of funds information from the bank, which was incorporated into the SAR filed by the online broker-dealer.

Using 314(b) Leads to Real Results for Law Enforcement

A clear example reiterating the value of the 314(b) program to law enforcement was highlighted in the October 2011 issue of *The SAR Activity Review – Trends, Tips & Issues*. A SAR review team proactively identified SARs totaling several million dollars. The SARs were filed by financial institutions that shared information on the subject under the auspices of the 314(b) program. Accounts were opened by the subject at the financial institutions with similar patterns of suspicious activities, leading the second institution to contact the first one through a 314(b) communication. The first institution had already filed a number of SARs on the subject. As a result of their communication, the requesting institution filed a SAR reporting activity on checks returned for insufficient funds, and included strong indications of fraud that pointed to a possible Ponzi scheme. After further investigation by law enforcement, the subject was charged with wire fraud and possession of counterfeit checks, ultimately pleading guilty to mail fraud and agreeing to pay more than $3.5 million in restitution.

Conclusion

The steady rise in 314(b) SAR filings underscores the recognition by financial institutions that the 314(b) process can significantly augment their internal due diligence and transaction monitoring efforts, enhancing their "Know Your Customer" efforts. Realizing that in many situations it may have only a small "piece of the puzzle," the financial institution utilizing 314(b) communications is able to reach out to other financial institutions to gather additional invaluable information on customers and/or transaction trails of mutual interest.

Instead of just the limited set of information that a financial institution may have on a customer or activity, the 314(b) participant can obtain information about new accounts, activities, associates, and/or segments of complex financial trails, of which it was previously unaware. The newly obtained information allows the requesting financial institution to build a more comprehensive and accurate picture of its customer's activities, providing for more accurate decision-making in the due diligence and transaction monitoring segments of its compliance efforts.

Moreover, incoming 314(b) requests alert the contacted financial institution to customers about whose suspicious activities it may not have been previously aware, and prompt the contacted institution to investigate further. A number of SARs in the study referencing 314(b) were filed not by the requesting institution, but by the contacted institution. Thus, the sharing of information benefits the due diligence and transaction monitoring efforts not only of the requesting institution, but the contacted institution as well.

314(b) communications have resulted in the filing of more comprehensive and complete SARs than would otherwise have been filed if the requests had not been made. SARs that reference 314(b) requests with positive results may provide a plethora of account, transaction, cross border financial trails, and/or identifying information about which the requesting (or receiving) institution had no prior knowledge. In some cases, both the requesting and the contacted financial institutions file SARs on the same suspects and their activities, when no SAR would have been filed in the absence of the 314(b) request. The 314(b) program, then, has proven invaluable to 314(b) financial institution participants initiating sharing requests, 314(b) participants responding to the requests, and the law enforcement and regulatory community.

For more information regarding participation in the 314(b) program, please refer to the program subsection of FinCEN's Web site at: http://www.fincen.gov/statutes_regs/patriot/section314b.html

Law Enforcement Cases

This section of *The SAR Activity Review* summarizes cases where FinCEN information played an important role in the successful investigation and prosecution of criminal activity. This issue contains new case examples from Federal and local law enforcement agencies. Additional law enforcement cases can be found on the FinCEN website under the link to "Investigations Assisted by BSA Data". This site is updated periodically with new cases of interest, which are listed by the type of form used in the investigation, type of financial institution involved, and type of violation committed.

Contributing editors: Shawn Braszo, Molly Jerome, Don Battle, Sean Evans, Sean Donnelly, Jim Emery, and Jack Cunniff.

In this edition, we highlight the use of BSA material, particularly SARs, by providing specific examples of how the detection and analysis of suspect transactions by financial institutions led to the prosecution of criminals in a wide range of cases. Several of our examples come from SAR review teams where law enforcement entities launched major investigations based on quality records filed by financial institutions. These investigations included illicit sales and the purchase of vehicles for drug smuggling. But even in cases not started by SARs, BSA records can greatly enhance an investigation. We provide case examples where this information proved critical in investigations such as drug trafficking, the smuggling of untaxed cigarettes, and elder abuse.

SARs Reveal Multi-Million Dollar Illicit Business

Through a proactive review of SARs, law enforcement found that the purveyor of illicit devices structured millions of dollars of proceeds into a financial institution. The devices were a violation of state law and hence led to a charge of money laundering. In the indictment, prosecutors sought almost $7 million in forfeiture.

A Federal jury found the defendant guilty of dozens of counts of structuring financial transactions and one count of money laundering. He also pled guilty to one count of running an illicit business, and received a sentence that included prison time. An associate was also implicated in the crime and sentenced to 1 year of home confinement with electronic monitoring.

The defendant's business sold illicit devices to retail establishments. He took the proceeds generated by these devices and split the profits with the establishments. The defendant then structured the deposits of these funds in order to hide his illicit business, the success of which allowed him to lead a luxurious lifestyle.

Despite his best efforts to hide his illicit banking activity, the defendant's operation was fully exposed because of filed SARs. An assistant United States attorney stated that the SARs initiated the investigation and were central to the prosecution's case. SARs were filed by a financial institution after numerous deposits into the account for the business. The original SAR noted that deposits ranging between $9,400 and $9,900 were being made regularly into the account over a period of several years. Additional SARs noted that the structuring activity continued, resulting in the institution closing the account. Altogether, the filed SARs showed that more than 500 deposits were made just below the $10,000 threshold for CTRs, with the defendant depositing more than $4 million in illegal proceeds.

The defendant's business ventures had drawn interest from law enforcement for years. A special agent, who found the SARs on the defendant during a proactive review, stated that the ability to levy structuring charges against the defendant was directly due to the BSA documents. Without the structuring charges, no case would have been made against him.

The defendant had at one point been designated as an exempt entity by the financial institution, but that exemption had been revoked. He tried to explain that he did not know about the revocation, and that is why he structured the transactions.

Suspicious Activity Report Helps in Investigation of Doctor Prescribing Thousands of Pain Relief Pills

A doctor who distributed more high powered pain pills than the largest regional medical center was brought to justice with the help of BSA records. In these types of investigations, proving that the prescriptions for pain relief are unwarranted can be very difficult because doctors often follow the letter of the law by seeing and listening to patients – although in very short sessions. However, a SAR detailed structuring that indicated additional financial crimes.

A Federal judge sentenced the defendant to several years in prison and years of supervised release for distribution of a controlled substance and structuring financial transactions. The doctor prescribed tens of thousands of one type of pain relief pills in less than a year. By contrast, over the same period the region's largest hospital ordered less than 20 percent of that number of tablets.

According to records filed in the case and statements in open court, investigators began examining the defendant's prescribing practices after numerous drug dealers were arrested with prescriptions the defendant had prescribed. Investigators sent a test patient into the clinic, who obtained a prescription for the powerful narcotic with only a cursory examination. The patient was also able to get the prescription renewed after subsequent visits that lasted about a minute. When investigators served a search warrant on the doctor's home, office, and storage unit, they found hundreds of thousands of dollars in cash that he had never declared on his tax returns. The doctor admitted attempting to deposit it in amounts below $10,000 to avoid bank reporting requirements. The defendant's plea agreement included a forfeiture of more than $1 million seized in the case. In requesting the multi-year prison term, prosecutors wrote to the court that as a medical professional the defendant knew far better than the typical drug dealer the dangers of the substances he was distributing.

As part of the investigation, analysts made several queries of the BSA records database over an extended period. During one query, they discovered a SAR filed by a financial institution that noted that in a 2-month period the doctor was responsible for more than 10 cash deposits totaling more than $94,000 in structured amounts. The discovery of the structuring indicated that he was making a lot of money and trying to hide it from the IRS. Interestingly, at some point the doctor became concerned about triggering a CTR and withdrew his money and closed the account at that financial institution.

According to the case agent, the existence of the SAR proved critical to the investigation. First, the record showed evidence of another criminal activity – structuring. Second, the SAR also showed the potential of tax violations. Law enforcement officials have found that prosecuting doctors on suspect prescriptions is often difficult because the doctors follow the technical aspects of the law when it comes to patient care. But in this case, the probable financial violations help generate enthusiasm for a robust criminal investigation.

The evidence of structuring helped secure a search warrant for the defendant's office. During that search, they found a statement of a business checking account from a local credit union. The credit union account had a balance of nearly $500,000 with more than $100,000 in structured deposits for the month and no withdrawals. Sensing that the account would be seized, the doctor withdrew most of the funds in the form of a cashier's check just before the investigators were able to seize the money. Agents eventually retrieved the check from the doctor's wife.

SARs Help Dismantle Inter-State Cigarette Smuggling Operation

A nationwide conspiracy to purchase cigarettes in the South and illegally sell them in Northern States resulted in the loss of millions of dollars in state tax revenue. In some cases, the unpaid tax on a carton of cigarettes was almost $40 a carton. Some of the conspirators made trips south to purchase the cigarettes, while other supplied the cigarettes, knowing they were for out-of-state sales. One defendant was found to be responsible of structuring the illicit payments into local banks.

The defendants pleaded guilty to various counts involving the purchasing, transportation, possession, and distribution of illegal cigarettes. Of note, one subject pled guilty to aiding and abetting structuring, another to aiding and abetting money laundering, and a third to aiding and abetting interstate transportation of stolen goods, money laundering, and aiding and abetting the counterfeiting of cigarette tax stamps.

As described in court documents, the conspiracy was carried out by defendants acting as both buyers and suppliers. The buyers repeatedly traveled, normally in one or more full-sized vans with out of state license plates, from the northeastern United States to the South for the purpose of purchasing large quantities of cigarettes outside the normal flow of commerce. The suppliers provided the contraband in exchange for cash payment. The buyers and suppliers would arrive at a predetermined time and place and complete the illicit transaction. The buyers would then return to the northeast to sell the smuggled cigarettes at a profit.

To avoid detection of the distribution of illegal cigarettes in the Northeast, the buyers dealt with and sometimes sold counterfeit tax stamps. Eventually, the buyers began using the counterfeit tax stamps to generate additional income or trading them for additional cigarettes.

The buyers often re-invested their profits from the scheme for cash purchases of additional cigarettes. Once the cash transaction took place, a supplier structured the proceeds into the banking system. He would make single deposits in amounts close to $10,000 and make multiple deposits on the same or successive days which totaled just below this limit, avoiding the filing of a CTR on the cash deposits. A financial institution filed several SARs on the defendant for structuring transactions. Through his legitimate business, he deposited large amounts of currency that frequently resulted in CTRs. However, prosecutors noted more than 150 additional suspicious structured transactions that were traced to complicity in the smuggling operation. That defendant was eventually warned by a bank official that his account

appeared to show a pattern of deliberate structuring to avoid the filing of CTRs. He acknowledged that he was aware of the structuring regulations and opened a new account in which to deposit profits from the scheme.

SARs Help Investigators Stop Fraudsters

Investigators opened a case after receiving a call from a family friend of a wealthy elderly woman who suspected the woman was being taken advantage of financially. With this information the law enforcement officials proceeded to research BSA documents and found SARs describing structuring on the part of the subjects acquainted with the woman.

One subject was sentenced to more than 1 year in prison, followed by multiple years of supervised release, for illegally structuring cash withdrawals to evade reporting income on his federal tax returns. Another defendant pleaded guilty to a similar charge and was given probation.

Investigators said that the defendants were both involved in a scheme which consisted of taking advantage of a wealthy elderly woman. The subjects used many tactics in order to receive money from her. One subject misrepresented himself as a former employee of the Federal government and convinced the woman that she needed protection from terrorists that were in the area. He proceeded to build a wall around the victim's property, convinced her to have a security system installed, and charged the woman tens of thousands of dollars for installation when the actual system cost a fraction of what she was charged. The men took care of her property, doing odd jobs, and ran errands for the woman. The elderly woman considered one defendant a trusted friend and included him in her will. She also continually loaned money to both subjects.

One defendant withdrew $2 million from the victim's account in cash and cashier's checks through 200 transactions, and pleaded guilty to trying to avoid triggering a CTR required by Federal law. The defendant also failed to file his taxes for several years. He claimed his preparer made a mistake and did not file the taxes.

Investigators opened the case when a friend of the elderly woman's family came to visit and discovered many checks written to the two men. When the friend questioned the woman about the checks she said the men did work for her around the property. The family friend notified officials who in turn spoke to the woman. At first she denied that they were committing any kind of crime but eventually investigators were able to convince her to some extent of the continuing crime taking place.

Investigators stated that BSA records were essential to the investigation. A SAR filed by a local financial institution noted that transactions appeared to be structured to avoid the filing of a CTR, while also describing the suspicious movement of funds. One defendant made large withdrawals in cash at various branches and also made multiple purchases of cashier's checks and cash withdrawals in the same transaction. A subsequent SAR noted similar activity.

Another SAR stated that 3 months of account history on the joint account of one defendant and his wife had been reviewed to determine that some activity is consistent with previous account history, but large cash deposits at various locations prompted the SAR. The source of the funds was unknown.

A third SAR stated that account history was reviewed to determine a change in the pattern of activity due to dramatic increases in cash deposits. That activity appeared to be structured to avoid the filing of a CTR. The customer deposited large amounts of cash at multiple branches, over a period of several days.

BSA Records Help Dismantle Oxycodone Ring

Members of a multi-state drug trafficking and money laundering organization have pled guilty to multiple counts of narcotics trafficking and money laundering. The organization trafficked in Oxycodone and the movement of large amounts of money between two states. The organization was identified over a number of years and through several investigative processes, but through the use of SARs investigators were able to identify and help dismantle key parts of the money laundering operation, in addition to the narcotics trafficking.

A local police department began the investigation several years earlier, but a lack of financial resources prevented the case from proceeding. However, the prosecutor eventually took a position with the U.S. attorney's office and was able to garner Federal resources to open another investigation.

The investigation and prosecution proved that the conspirators used several methods of transporting narcotics, primarily painkillers. Members of the organization used commercial flights, couriers, and package delivery services to transport large quantities of narcotics and monetary proceeds from narcotics trafficking. The prosecuting assistant U.S. attorney stated that the organization was involved in the trafficking narcotics worth millions of dollars. Records indicate that at least $1 million existed in the combined bank accounts of three conspirators, and that at least 11,000 pills had been distributed during the commission of the conspiracy.

Investigators believe that much of the Oxycodone originated through the sale of legitimate prescriptions or the creation of false prescriptions. Then, through the use of one of the above-mentioned methods, the Oxycodone was shipped, distributed, and sold for profit. In several instances, one defendant admitted to depositing the proceeds from this distribution to a credit union account owned by a co-conspirator. That individual then claimed the money in business receipts for a fraudulent tour business.

BSA data had been collected on several individual suspects in the case. A review of SARs by investigators indicated a complex system of money laundering and structuring over the course of several years. The lead prosecutor of the case indicated that the SARs were instrumental to the investigation due to the fact that the majority of the proceeds stemming from the narcotics trafficking were in cash and would not be otherwise traceable. The prosecutor also noted that the investigation focused on a method of attempting to dismantle the organization by "starting at the head". In this sense, the SARs became necessary in identifying who was transferring and was responsible for the largest amounts of money.

Suspicious Activity Reports were filed proactively by banking institutions before the investigation came to their attention. SARs were filed in both states, and financial intelligence units within several banks and credit unions provided follow-up investigative support and filed additional SARs when necessary.

One defendant was identified by several SARs and CTRs filed by a credit union. According to the SARs, the defendant identified himself to banking institutions as a tour guide operator, and structured well over $300,000 through the credit union. An early SAR indicates that the defendant attempted to avoid reporting requirements by depositing under $8,000 at the bank, and then returning later in the day to deposit $3,000 at the ATM. When he was made aware that such a transaction would require a CTR to be filed, the defendant refused to do so and indicated that he was previously aware of CTRs. For this reason the credit union filed SARs proactively and initiated several 90-day follow up investigations into his account.

A SAR filed on another defendant, identified as the account holder, exhibited a pattern of structuring thousands of dollars in $3,000 increments over a one-month period into and out of the account. The transactions occurred at a money services business and it is believed by investigators that the money being transacted eventually went to a second defendant, who then attempted to launder the proceeds through his fraudulent company.

A third defendant, who ran a personal training business, was also the subject of several SARs and CTRs. The records indicate that the defendant transacted well over $300,000 throughout the course of the criminal conspiracy, and much of this money likely went to the co-conspirators as profit. The SARs revealed that the defendant frequently made rapid deposits and withdrawals out of a checking account in the defendant's name, and rarely provided indicators of where the money was coming from or going to. That defendant additionally patterned these deposits and withdrawals in a manner designed to evade reporting requirements. The financial institution could not determine any legitimate reasons for the frequency of these transactions based on the defendant's listed employment.

The conspiracy began to unravel when police arrested a courier with a significant amount of Oxycodone pills. The courier agreed to assist in a controlled-buy of the narcotics, and two co-defendants were arrested as a result. Later, police intercepted a package of narcotics and tracked it to two other co-defendants who were being tried separately. As the number of arrests grew, one defendant fled while the rest of the immediate group was arrested. The defendant was later arrested by U.S. Marshals.

SARs Help Bust $1 Million Drug Ring Led by Significantly Older Student

SARs helped Federal investigators unravel a cross-country drug trafficking ring centered around a large urban university campus. The case featured shipments of marijuana and subsequent large currency deposits and withdrawals designed to avoid reporting requirements. Notably, a financial institution identified structured deposits on the East coast and near simultaneous withdrawals at other locations across the country. Investigators and prosecutors noted how helpful BSA records were to the investigation.

A Federal judge sentenced the defendant to more than 15 years in prison after his conviction for running a marijuana ring that produced over a million dollars in drug proceeds. The defendant started shipping high-grade marijuana from his hometown on the West coast to distributors based around an eastern university campus where the defendant, some 20 years older than his peers, was registered as a student. With the utilization of SARs filed on both coasts, Federal agents were able to discover and confirm the identities of drug-smuggling individuals, as well as other parties, involved in this large trafficking scheme.

Prior to the establishment of the drug ring, the defendant had a history of felony and misdemeanor charges. A large number of the previous charges centered on the possession and distribution of drugs. The defendant was charged with

felony possession of cocaine, as well as DUIs in three different states. A further examination of his criminal records reveals multiple assault charges, frequently with deadly weapons resulting in injury. Altogether, over the period covering more than a decade, authorities charged the defendant with a combination of nearly 40 misdemeanors and felonies.

The case started when Federal investigators confronted and "flipped" one of the defendant's main dealers and began to build their case against him and his associates. Because the defendant and his associates structured hundreds of thousands of dollars into bank accounts to avoid the filing of CTRs, those transactions prompted a financial institution to file SARs for the activity that occurred on both coasts. With these SARs, agents were able to confirm that defendant received cash proceeds while near his home from his dealers selling marijuana at the university. In the SARs, the financial institution noted the large deposits of cash on the East coast coincided with large withdrawals of cash in the West. Bank surveillance photos taken at the time SARs were filed show footage of the defendant structuring withdrawals in a manner that was coordinated with the structured deposits taking place on the other side of the country. One SAR detailed transaction activity encompassing just over a year and totaling more than $375,000. Of these more than 140 total deposits, nearly 80 percent of them accounted for more than $350,000 in currency. In fact, currency made up more than 90 percent of all funds deposited. Of the deposits that appeared to be currency, more than a dozen were in the $8,000 to $10,000 range, and none were in the $10,000 to $12,000 range, which would have required the filing of CTRs.

This same SAR detailed the structuring of numerous cash deposits and withdrawals that took place during one week. In that five-day period, a dealer in the East made several structured deposits which totaled more than $75,000. Simultaneously, the defendant made several structured withdrawals in the West totaling just under $70,000. Despite the large amount of the cash flow, none of the deposits or withdrawals exceeded $10,000.

The cooperative structuring in the same bank account between these two men confirmed a business relationship based on money laundering. Other SARs filed during this period linked fellow drug dealers with the drug trafficking organization, detailing similar drug-related financial transactions.

Through the SARs, the financial institution helped supply authorities with needed information regarding the trafficking organization. According to the lead prosecutor in this case, the BSA data served to connect good intelligence with underlying structuring that tied identities to the other party's financial transactions.

SARs Help Uncover Scheme to Hide Payments from Drug Traffickers to Buy Vehicles

A vehicle dealer created a scheme to hide payments for the purchases of aircraft by suspected drug traffickers. The scheme involved using multiple bank branches for deposits, and the avoidance of filing any Form 8300s. However, the alert financial institution identified the suspect transactions and filed multiple SARs. A SAR review task force identified the relevant SARs and initiated an investigation.

The investigation resulted in the corporation that sold the vehicles pleading guilty to conspiracy to aid and abet structuring financial transactions. The owner and president spoke on behalf of the company at the plea hearing, admitting the factual basis for the plea was accurate.

As admitted in court, the corporation sold multiple vehicles for cash to purchasers whom they believed to be foreign nationals, involving deposited cash they believed to be from illegal narcotics trafficking. The company and its agents knew that the buyers were structuring cash into the corporate account in increments of less than $10,000 in order to avoid Federal cash transaction reporting requirements.

The company and its agents tracked deposits by these purchasers, requiring them to alert the corporation of the deposits and which vehicle sales the deposits related to. Often the purchasers faxed cash deposit tickets to the corporation as proof to ensure credit for the payment. They made deposits in such a way that the banks could not connect the transactions to a specific buyer or vehicle, and could not identify the individuals making the deposits or purchasing the vehicles, and therefore could not file a CTR for large cash transactions.

An undercover agent made contact with the owner stating that he wished to purchase a vehicle for a relative with currency and asked for advice on how to accomplish that without having any reports filed on the cash transaction. The owner's response indicated that he understood that the relative was engaged in drug trafficking activity in a foreign country, specifically trafficking marijuana. The owner proceeded to advise the agent how the foreigners did it, depositing cash in increments into corporate accounts and a salesman advised the agent about the corporation's Form 8300 reporting requirement for such cash transactions. When the owner asked how they got away with not reporting the foreigners, the salesman advised that no one had ever hassled the corporation about the issue. In a period of nearly one year, the corporation received nearly $500,000 in structured funds for several planes, each with a separate buyer.

Several years earlier, a financial institution filed a SAR noting that the salesman came into a branch with more than $170,000 to deposit in currency, claiming that the client did not have time to wire the money. The client, who accompanied the salesman to the bank, showed documentation that he was a resident and citizen of a foreign county. The financial institution filed subsequent SARs, especially in the years relevant to the criminal actions outlined in the plea agreement. For example, one SAR notes deposits into branches throughout several states from unknown sources.

The case started when a proactive SAR review team identified one of the SARs filed on the owner. Undercover operations confirmed that the subjects were willing to circumvent reporting requirements, and had no problems selling the vehicles to potential smugglers, as long as the planes were only going to be used to smuggle marijuana.

SAR Leads to Guilty Plea for Used Car Dealer Willing to Launder Drug Proceeds

A used auto dealer pleaded guilty to laundering $35,000 in currency from an undercover source acting on behalf of Federal agents. The investigation, initiated by a SAR, led to the arrest of the subject.

A SAR showed excessive cash activity in the account for the used car dealer, with the filer noting that there was an unusually large cash amount for a used car dealership and that they suspected the business of money laundering. Concurrently, law enforcement agents received an anonymous tip suggesting that the defendant was involved in money laundering or bulk currency smuggling. With this information and the SAR, the Federal agents began a year-long investigation into the subjects.

At one point, the defendant sold a vehicle to a confidential source working at the direction of law enforcement. The source represented himself to the defendant as a narcotics dealer paying for the vehicle with proceeds from narcotics dealing. The source paid the defendant approximately $13,000 for the vehicle. Prior to the sale, the source and the defendant discussed the reason for needing a vehicle and the source said it was for narcotics trafficking. At the time of the sale, the defendant provided the confidential source with a purchase agreement and bill of sale for the vehicle that did not list the source's name so that the purchase could not be traced to him. A few days later, the defendant had one of his employees prepare the paperwork for the sale of the vehicle. Prior to the sale, the defendant and the source came to an agreement to list the sale of the car as $9,000, rather than the actual sale price, to avoid any cash transaction reporting requirements that the defendant knew would arise in a transaction of $10,000 or more.

A few months later, the defendant sold another vehicle to the source, once again taking measures to avoid cash reporting requirements and hiding the identity of the buyer. The defendant reported the cost of the vehicle to be $9,500 instead of an actual cost that was in excess of $10,000. Before the sale of the vehicle, the source requested that a hidden compartment be installed for the smuggling of narcotics. The defendant facilitated this request through a car customizer that he was acquainted with.

On another occasion, the defendant accepted a large cash down payment from the source for the purchase of two more vehicles. The actual price of each vehicle was over $10,000. The source once again told the defendant that the funds used for purchasing the vehicles were proceeds from a drug sale. The defendant again planned to under-report the price of the vehicles so as to avoid reporting procedures.

The prosecutor reported that BSA information led them to the target and gave law enforcement an avenue through which to initiate the investigation.

Usage of BSA Data

"The Federal Bureau of Investigation reports that, as of June 2012, 37 percent of their pending counter-terrorism cases have associated BSA records, and more than 90 percent of those counter-terrorism BSA records are CTRs."

Source: FinCEN Director Jennifer Shasky Calvery, in a speech before the Florida International Bankers Association, (February 13, 2013).

Issues & Guidance

This section of *The SAR Activity Review* discusses current issues, including those related to the preparation and filing of SARs, and provides guidance to filers.

A Message from the Office of Financial Protection for Older Americans, Consumer Financial Protection Bureau

By the Consumer Financial Protection Bureau

On the occasion of Older Americans Month this May, the Consumer Financial Protection Bureau's Office of Financial Protection for Older Americans (Office for Older Americans) welcomes FinCEN's efforts to encourage the reporting by financial institutions of suspected elder financial exploitation. FinCEN's update of the SAR with a designated reporting field for elder financial exploitation is an important step forward. Financial institutions' use of SARs to report suspicious activities in the transactions and accounts of older adults will focus attention on the need to protect older consumers, increase law enforcement use of SARs to investigate cases of suspected elder financial exploitation and collect much-needed data on the prevalence and types of financial abuse.

The CFPB's Office for Older Americans looks forward to working with FinCEN to raise the awareness of the use of the SAR and of these devastating crimes that threaten the economic stability of older Americans. The Office for Older Americans has a broad mandate that includes working to improve financial literacy of individuals aged 62 years and over and developing strategies to protect them from unfair, deceptive, and abusive financial practices.

To this end, we are coordinating with federal agencies through the Elder Justice Coordinating Council and are developing several tools for older adults, caregivers and advocates including:

- plain-language guides for "lay fiduciaries" – family members and other non-professionals who handle finances for older adults with diminished capacity
- a community awareness program on how to identify, prevent and report fraud, scams and other forms of elder financial exploitation, and

- a strategy for communicating clearly to financial institutions that Federal law generally permits them to report suspected abuse to—or respond to requests for personal information from—law enforcement, Adult Protective Service Agencies, and other relevant entities.

Once released, we will seek to disseminate these publications and tools throughout the public and non-profit sectors.

CFPB welcomes this opportunity to highlight our work to prevent elder financial exploitation and to acknowledge the work of our sister Federal financial regulators as well as financial institutions to protect older consumers.

SAR Narrative Key Terms: Updated Guidance on the Use of SAR Check Box Items

By FinCEN's Office of Outreach

FinCEN's website contains a consolidated listing of Suspicious Activity Report (SAR) Key Terms and a link to the related FinCEN advisory/other publication related to each key term. This list is updated when new advisories are published and was most recently updated on February 26, 2013.

The FinCEN SAR (available only on the BSA E-Filing System) now contains check box items for some of the key terms contained in the consolidated list. In the table below, we have identified 1) the key terms that now have a check box item on the SAR, and 2) the corresponding check box item that will suffice for identifying the suspicious activities. Institutions may still include the key term in the narrative section, but we will no longer request that it be included in the narrative section if a check box item exists for the key term.

Narrative Key Term	***Corresponding SAR Check Box Item***
TBML (Trade Based Money Laundering)	Item 33 (k) Trade Based Money Laundering/ Black Market Peso Exchange
BMPE (Black Market Peso Exchange)	Item 33 (k) Trade Based Money Laundering/ Black Market Peso Exchange
account takeover fraud	Item 35 (a) Account takeover
elder financial exploitation	Item 35 (d) Elder financial exploitation
foreign corruption	Item 35 (l) Suspected public/private corruption (foreign)
IVTS (Informal Value Transfer System)	Item 35 (m) Suspicious use of informal value transfer system

Industry Forum

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into an aspect of compliance management or fraud prevention. The information provided and opinions expressed may not represent the official position of the U.S. Government.

FinCEN SAR Checkbox for Human Trafficking

By Joann Alicea, Senior Risk Analyst, PreCash

Modern-day slavery

Human trafficking is a crime that has become the second largest criminal enterprise in the world, with an estimated 27 million people currently enslaved worldwide. It has passed the illegal arms sales in the global black market trade.[45] Human trafficking victims include men, women and children in labor servitude, private ownership and in sexual services. Human trafficking is a form of modern-day slavery where people profit from the control and exploitation of others. We can help fight child pornography and child exploitation as children are being sold for sex trafficking on the Web at various Internet ad sites. This is why I am lobbying for a SAR checkbox to be added for the money trail reporting of the horrific crime of human trafficking.

Human Trafficking is big business

The crime of human trafficking is big business because it yields an estimated $32 billion in illicit profits each year. Unlike drugs and arms traffickers, human traffickers can continue to exploit their victims after the initial point of sale. When you or I go to the store and purchase an item, the goods we buy are a one-time purchase and we are done with the buying. A human being sold is reusable – for sale over and over again until they are either rescued from the trafficker, escape on their own or die. Human trafficking is a market-based economy that exists on the principal of supply and demand.[46]

45. http://www.weaveinc.org/post/facts-about-human-trafficking
46. http://www.ricw.ri.gov/Human%20Trafficking/index.php

FinCEN Suspicious Activity Reports

AML investigators are aware that *18 U.S.C. § 1956 : Laundering of monetary instruments* includes in its "specified unlawful activities" in section(vii) that trafficking in persons, selling or buying of children, sexual exploitation of children, or transporting, recruiting or harboring a person, including a child, for commercial sex acts" is illegal.[47] Thus, criminals engaging in these online postings who generate funds from such activities are susceptible to money laundering prosecutions. Identifying a site as possibly being used for such heinous activities, however, requires us to have enhanced knowledge about these sites, so that we can better file Suspicious Activity Reports. SARs can and should be used to report transactions that may be being used for suspected human trafficking whether it be slave labor or sex trafficking. Unfortunately, the current SAR form lists fraud, money laundering, terrorist activity, but does not contain a separate check box for human trafficking. It is time that the SAR form is updated to include human trafficking that can be advertised through Internet Web sites being paid for through our financial systems.

Until the form is updated to identify human trafficking as a predicate offense to money laundering, SAR preparers can continue to use the "Other" box; and ensure that key words are included in the Part V Narrative text. In this regard, as well, it would be useful to work with key phrases that could be included in the narrative on which law enforcement could search for the SAR review terms, and others potentially targeting the trafficking of children. Another recommendation is that FinCEN issue an alert with suggested "Narrative text" language to use in filing a SAR that can be tracked by SAR review teams. Our current inability to call out Internet human trafficking specifically as the suspected predicate offense does its victims a great disservice.

Disturbing facts

- Approximately 55 percent of American girls living on the streets engage in the commercial sex trade[48]
- For every 800 people trafficked only 1 person is convicted[48]
- A young girl can earn between *$150,000 and $200,000 each year* for her pimp if she survives[48]
- Two million **children** are bought and sold in the global commercial sex trade annually[48]

47. http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00957.htm.
48. http://higherlogicdownload.s3.amazonaws.com/ACAMS/e91557e6-bbb6-4fc9-9b7c-eef66256706a/UploadedImages/pdf%20downloads/Chapters/Houston/ACAMS%20PUBLISHED%20$5.00%20TO%20RUIN%20THE%20LIFE%20OF%20CHILDREN%20AND%20WOMEN.pdf.

- The average American girl is 13 years old when she is forced into commercial sex slavery [48,49]
- Victims of sex trafficking are also victims of gang rape[50]
- Experts estimate that as much as **76 percent** of transactions for sex with underage girls are processed through **Internet ads**.[51]

Our responsibility: Following the money trail

It is a responsibility of the AML and financial investigative professional to police financial systems to ensure that, in no way, are our financial systems being employed to finance the commercial sex trade of minors via Internet ads. It is our job to identify and appropriately report predicate offenses to money laundering. Sex with a minor is illegal and any proceeds resulting from this activity would be tainted. Likewise, prostitution is illegal in most jurisdictions. Placing the tainted proceeds into the financial system would constitute money laundering and would thus be SAR reportable. Stopping the flow of money for the illegal advertising of children for the sale of sex on various Internet ad sites will help to undercut the Internet based commercial sex trade in the U.S. However, the job is not complete until all financial institutions and non-financial institutions with card-based products have monitoring systems in place to identify red-flags for Internet prostitution sale or purchase. It must be understood that the criminal suppliers and the criminal purchasers will not stop this activity until their methods of payment is taken away from them. When these channels are plugged, the criminals will simply move on to the next unsuspecting credit card or pre-paid card offering.

In conclusion, we as a team of professionals that utilize the FinCEN SAR can assist in the fight to help stop the selling and buying of girls and women on Internet ad sites by using the financial tools we have to cancel all suspicious activity and report the activity through an updated SAR reporting process that includes a new SAR form with a check box for human trafficking.

---

49. http://cnnpressroom.blogs.cnn.com/2011/01/18/cnn%E2%80%99s-amber-lyon-investigates-teen-trafficking-in-america/
50. www.polarisproject.org/human-trafficking/human-trafficking-faqs
51. www.prnewswire.com/.../craigslist-ads-featuring-adolescent-females-...

Feedback Form

Financial Crimes Enforcement Network

U.S. Department of the Treasury

Tell Us What You Think

Your feedback is important and will assist us in planning future issues of *The SAR Activity Review*. Please take the time to complete this form. The form can be faxed to FinCEN at (703) 905-3885 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 (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

Money Services Business:
__ Money Transmitter
__ Money Order Company or Agent
__ Traveler's Check Company or Agent
__ Currency Dealer or Exchanger
__ Prepaid Access

Securities and Futures Industry:
__ Securities Broker/Dealer
__Futures Commission Merchant
__Introducing Broker in Commodities
__Mutual Fund

Casino or Card Club:
__ Casino located in Nevada
__ Casino located outside of Nevada
__ Card Club

__ **Insurance Company**
__ **Dealers in Precious Metals, Precious Stones, or Jewels**
__ Non-Bank Residential Mortgage Lender or Originator
__ **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				
Trends and Analysis	1	2	3	4	5
Law Enforcement Cases	1	2	3	4	5
Issues & Guidance	1	2	3	4	5
Industry Forum	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):

_____
_____
_____
_____

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

_____
_____
_____
_____

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, for example: information on a certain type of activity, or an emerging technology of interest.

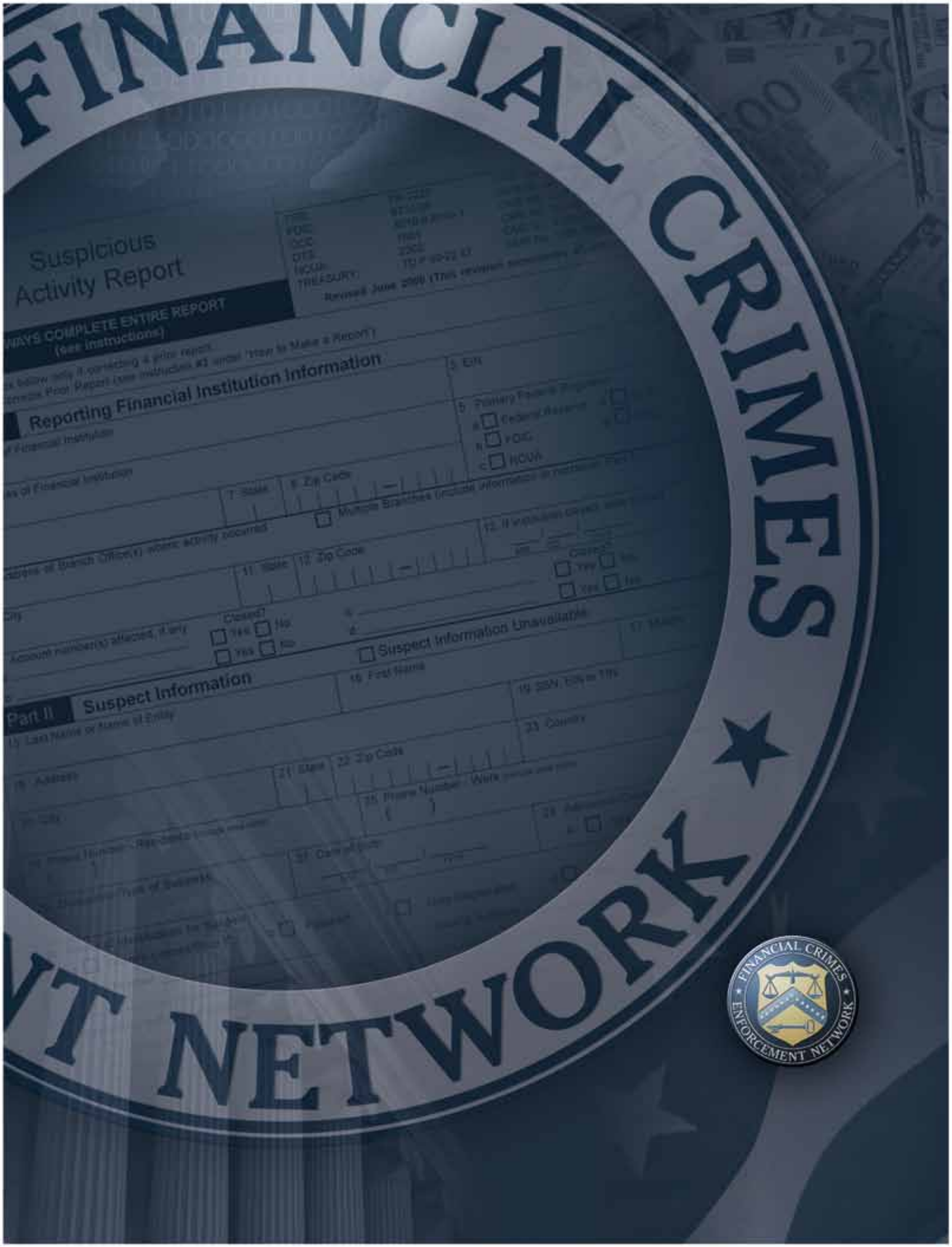
_____
_____
_____
_____

F. What other feedback does your financial institution have about The SAR Activity Review publication itself?

_____
_____
_____
_____

G. How often do you read the SAR Activity Review? (Check all that apply)

[ ] Every Issue
[ ] Occasionally
[ ] Only issues with content directly applicable to my industry or area of interest


FINANCIAL CRIMES
Suspicious
Activity Report
Reporting Financial Institution Information
Suspect Information
Suspect Information Unavailable
VT NETWORK
FINANCIAL CRIMES ENFORCEMENT NETWORK