

The background features a large, semi-transparent watermark of the FBI Financial Crimes Enforcement Agency (FinCEN) seal. The seal is circular and contains the text "FINANCIAL CRIMES ENFORCEMENT AGENCY" around the top and "FEDERAL BUREAU OF INVESTIGATION" around the bottom. In the center of the seal is a globe with binary code (0s and 1s) overlaid on it. The text "ADMINISTERING BANK SECRECY ACT THROUGH GUIDANCE" is written along the left side of the inner circle, and "ANALYZING BANK SECRECY ACT DATA TO IDENTIFY TERRORISM" is written along the right side. A five-pointed star is visible on the left side of the seal.

Issue 9

October 2005

The SAR Activity Review

Trends, Tips & Issues

The SAR Activity Review

Trends
Tips &
Issues

Issue 9

Published under the auspices of the Bank Secrecy Act Advisory Group

October 2005

Table of Contents

Introduction	1
Section 1 - Director’s Forum	3
Section 2 - Trends and Analysis	
Suspicious Activity Reports for Securities and Futures Industries.....	5
Computer Intrusion Violations within Depository Institutions.....	15
Section 3 - Law Enforcement Cases	
Investigations Assisted by Suspicious Activity Reports	31
Section 4 - Tips on Suspicious Activity Report Form Preparation & Filing	
Suspicious Activity Report Form Completion Tips – A trend analysis of frequently asked questions received on FinCEN’s Regulatory Helpline.....	39
Section 5 - Issues & Guidance	
Providing Suspicious Activity Reports to Appropriate Law Enforcement.....	43
Section 6 - Industry Forum	
USA PATRIOT ACT’s Full Weight Placed on Securities Firms.....	47

Section 7 - Feedback Form.....55

**Appendix - Index of Topics from Current and Previous Editions
of *The SAR Activity Review – Trends, Tips & Issues***

Introduction

The SAR Activity Review - Trends, Tips & Issues is a product of continuing dialogue and close collaboration among the nation's financial institutions, law enforcement officials, and regulatory agencies¹ to provide meaningful information about the preparation, use, and value of Suspicious Activity Reports filed by financial institutions.

Continuing with our new publication schedule, Issue 9 is the second of three issues of *The SAR Activity Review-Trends, Tips & Issues* that will be published in 2005. The Financial Crimes Enforcement Network (FinCEN) has received positive feedback from its readers concerning the new design, and we want to encourage all of our readers to provide feedback about the publication.

This edition identifies current trends in the securities and futures industries, as well as examines the emergence of the "Computer Intrusion" violation amongst depository institutions. Additionally, this issue provides guidance on disseminating Suspicious Activity Reports to law enforcement as well as tips on completing Suspicious Activity Reports. Below is a detailed view of topics discussed in this issue.

- Section 1: Director's Forum;
- Section 2: Trends and Analysis - Suspicious Activity Reports related to computer intrusion and Suspicious Activity Report filing trends in the securities and futures industries;
- Section 3: Law Enforcement Cases - summaries of Suspicious Activity Reports used in criminal investigations;
- Section 4: Tips on Form Preparation and Filing – the top questions

¹ Participants include, among others, the American Bankers Association; Independent Community Bankers of America; American Institute of Certified Public Accountants; Securities Industry Association; Futures Industry Association; Non-Bank Funds Transmitters Group; Board of Governors of the Federal Reserve System; Office of the Comptroller of the Currency; Federal Deposit Insurance Corporation; Office of Thrift Supervision; National Credit Union Administration; U.S. Securities and Exchange Commission; Commodity Futures Trading Commission; U.S. Department of Justice's Criminal Division and Asset Forfeiture & Money Laundering Section and the Federal Bureau of Investigation; U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement and U.S. Secret Service; U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence, Internal Revenue Service, and the Financial Crimes Enforcement Network.

received by FinCEN's Regulatory Helpline related to proper preparation of Suspicious Activity Reports;

- Section 5: Issues and Guidance - guidance for providing Suspicious Activity Reports to appropriate law enforcement entities;
- Section 6: Industry Forum - insight from one of our industry partners about the impact of the USA PATRIOT Act on the securities industry;
- Section 7: Feedback form.

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

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

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

Nona S. Tiedge
Assistant Director
Office of Regulatory Support
Analytics Division
Financial Crimes Enforcement
Network (FinCEN)
(703) 905-3968 (phone)
(703) 905-3698 (fax)
Nona.Tiedge@fincen.gov

Section 1 - Director's Forum



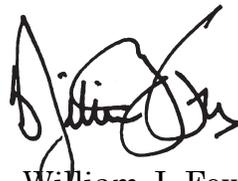
In the last edition of *The SAR Activity Review*, I highlighted the anxiety in the financial community over Bank Secrecy Act compliance expectations generally, and the filing of Suspicious Activity Reports in particular. I concluded with the unremarkable proposition that consistency, both in the interpretation of the Bank Secrecy Act and in compliance examinations, is the lynchpin to alleviating this anxiety.

On June 30, the federal banking agencies, in consultation with the Financial Crimes Enforcement Network, took a major step toward achieving this consistency with the collaborative development and release of the Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Examination Manual for banking organizations, including commercial banks, savings associations, and credit unions. The level of cooperation achieved in the development of this manual was unprecedented and represents the best of government. Independent agencies worked together to better ensure the uniform application of the Bank Secrecy Act. This examination manual is unique for another reason. In addition to examination procedures, it also includes a comprehensive resource of Bank Secrecy Act and anti-money laundering guidance. We expect this to be of great value to industry as well as examiners. Also, with the assistance of the Office of Foreign Assets Control, the manual contains procedures for examining financial institutions for compliance with our nation's economic sanctions laws.

The suspicious activity reporting sections of the manual appropriately place the focus of examiners on the policies, procedures, and processes that financial institutions have to identify, research, and report suspicious activity, rather than focusing on individual filing decisions. By focusing on systems, we ultimately seek to maximize the quality of the information reported and thereby maximize the utility of suspicious activity reports to the law enforcement, intelligence, and regulatory agencies that rely on these reports. Moreover, the manual confirms our understanding that, as a practical matter, it is not possible for a financial institution to detect and report all potentially illicit transactions.

This manual will not answer every question, and it certainly does not mean that we are finished providing guidance on Bank Secrecy Act compliance. The manual itself is a living document, something that we intend to update and adjust as necessary. Beyond that, we have numerous mechanisms and vehicles, such as the Bank Secrecy Act Advisory Group, through which we will continue to identify and address Bank Secrecy Act interpretive and examination issues. Finally, as the administrator of the Bank Secrecy Act, I look forward to working with my colleagues in the other federal and state regulatory agencies that examine financial institutions for compliance with the Bank Secrecy Act to use this manual as a model for achieving the same consistency across financial industries.

I would like to take this opportunity to wish a very good friend well in his new endeavors. As many of you know, John Byrne of the American Bankers Association is moving on to a new position as a Senior Vice President of Anti-Money Laundering Strategies at Bank of America. I would like to acknowledge and thank John for his significant contributions to our nation's anti-money laundering efforts over the years. I look forward to continuing to work closely with John in his new position and as he continues to co-chair the Bank Secrecy Act Advisory Group's SAR Feedback Subcommittee.

A handwritten signature in black ink, appearing to read 'William J. Fox', with a stylized flourish at the end.

William J. Fox
Director, Financial Crimes
Enforcement Network

Section 2 - Trends and Analysis

This section of *The SAR Activity Review* provides examples and patterns identified in suspicious activity reporting by both depository and non-depository institutions. This section addresses suspicious activity reporting related to the securities and futures industries as well as Suspicious Activity Reports related to the “Computer Intrusion” violation.

Suspicious Activity Reports for Securities and Futures Industries

Brokers and dealers in securities were required to report suspicious activity beginning in January 2003.² In May 2004, futures commission merchants and introducing brokers in commodities were added to the regulatory definition of “financial institution,” thus requiring them to comply with the recordkeeping and reporting obligations of the Bank Secrecy Act.

In Issue 7 of *The SAR Activity Review*, FinCEN reported on trends after the first year of mandatory filings.³ The following is an analysis of reporting by the securities and futures industries from January 2003 through June 2005.⁴ The analysis reviews the total number of filings, suspicious activities, occupations, violation amounts, and instruments used to conduct the suspicious activity. It also examines the types of institutions reporting, evaluates the geographic location of the filers, and takes an in-depth look at narratives.

Filing Trends

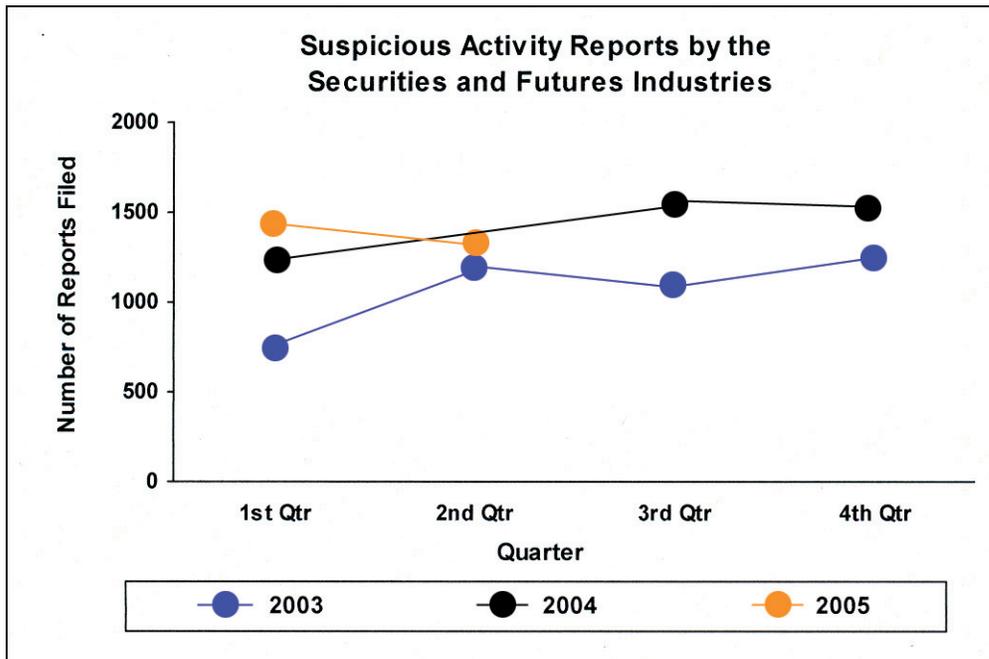
In its first year (2003), the securities and futures industries filed 4,267 Suspicious Activity Reports. In 2004, filings increased to 5,705 Suspicious Activity Reports. Current filing levels in 2005 are likely to meet or exceed the filing rate established in 2004. The chart below illustrates the filing trends over the last two years.

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

³ See <http://www.fincen.gov/sarreviewissue7.pdf>, page 20. Please note that futures commission merchants and introducing brokers in commodities were not required to report suspicious activity until after the period subject to review in Issue 7 of *The SAR Activity Review*.

⁴ Please note: Futures commission merchants and introducing brokers in commodities were not required to report suspicious activity until May 2004, although the analysis for this study dates back to January 2003.

Chart 1. Quarterly Filing Trend



Institutions Reporting

There is a variety of financial institutions filing Suspicious Activity Reports in the securities and futures industries. While many of the institutional categories identified on the Suspicious Activity Report form (in item 51) are not mutually exclusive, the majority of the institutions are self-identified as either clearing securities brokers or introducing securities brokers.

Instruments Reported

“Cash and cash equivalents” remains the most commonly reported instrument involved in a suspicious activity and is frequently cited in conjunction with the Money Laundering/Structuring violation within the securities and futures industries.

In 2004, there was a slight, but noticeable, fluctuation in stocks reported as the instrument involved in a suspicious activity. In the first quarter of 2003, stocks represented 2.54% of the securities and futures industries filings. By the second quarter of 2003, stocks reported as the instrument involved in a suspicious activity rose to 8.70% and then to 10.65% in the first quarter

of 2004. The percentage of reports that indicate stocks as the instrument involved continues to fluctuate around 10.65%. The increase between the first quarter of 2003 and the first quarter of 2004 may be due to a better understanding by broker-dealers of their Suspicious Activity Report filing obligations; or the increase may be the result of the economic recovery and subsequent rebound of the broad financial markets.⁵

**Table 1
Instruments Identified in
Suspicious Activity Reports filed by
Securities and Futures Industries**

Instrument	Count
Cash or equivalent	6591
Other	2578
Stocks	1597
Instrument description (check)	1082
Mutual fund	716
Money market fund	594
Market traded	385
Bonds/Notes	330
Other securities	136
Other non-securities	68
Foreign currencies	39
Commodity type	22
Security futures products	19
Commercial paper	19
Commodity futures contract	16
Other derivative	15
OTC derivative	14
Commodity options	13
Warrants	7
Foreign currency futures	4
Instrument description	0

⁵ A financial market is a market for a financial instrument, in which buyers and sellers find each other and create or exchange financial assets. Sometimes these are organized in a particular place and/or institution, but often they exist more broadly through communication among dispersed buyers and sellers over long distances.

Reviews of Suspicious Activity Report narrative sections were necessary to determine the nature of instruments associated with filings listing “Other.” The narratives indicate that “other” has become a catch-all receptacle for filings regarding negotiable instruments, such as drafts, checks, and guarantee instruments. In theory, these instruments can be coded as cash equivalents, but filers appear to be more comfortable listing them separately. Moreover, they are more likely to provide specifics about the nature of the abuse in the narrative section if the instrument is listed separately from “cash or cash equivalents.”

Suspect versus Filer Locations

Not surprisingly, the city/state distributions of securities and futures institutions filing Suspicious Activity Reports reflects many of the primary financial districts within the United States. As expected, more filers indicate an address in New York than in any other state, followed by Massachusetts, California, Washington, and Minnesota respectively.

In contrast, the distribution of the addresses for suspects was highly correlated to the 2000 United States Census, i.e., suspects in this group mirrored the general population with respect to location.

However, when the reporting branch location was not proximate to a suspect’s address, the Suspicious Activity Report most likely involved online brokerage activities. Straw accounts⁶ and funding fraudulent schemes were commonly reported. In these filings, there was no proximity between the addresses of the suspect and the branch reporting the suspicious activity. This association between suspect and filer locations was most obvious in filings reporting broker-dealers operating online businesses. In some instances, it appears that broker-dealers operating online have a straight-through application process: it involves a non-documentary means of customer identification, typically by checking credit bureau headers; therefore no official government identification is reviewed as a source document to verify applicant identity. Accounts that are opened without face-to face contact may be a higher risk for money laundering and terrorist

⁶ A straw account is established by someone presenting himself/herself as a straw man. The term straw man can refer to a third party that acts as a “front” in a transaction (i.e., one who is an agent for another) for the purpose of taking title to real property, breaking a joint tenancy, or engaging in some other kind of transaction where the principal remains hidden or who plans to do something else which is not allowed. A straw man is also “a person of no means,” or one who deliberately accepts a liability or other monetary responsibility without the resources to fulfill it, usually to shield another party.

financing, e.g., it is more difficult to positively verify the individual’s identity, customer may be out of the broker-dealer’s targeted geographic area or country, transactions are instantaneous, and accounts may be used by a “front” company or unknown third party.

Violation Amounts

The most commonly reported violation amounts in the securities and futures industries were in the \$10,000 to \$49,999 category. Reported violation amounts ranged from zero (\$0) to \$2.1 billion; generally, higher dollar amounts reported were associated with Advance Fee Fraud email solicitations as opposed to actual transactional amounts.⁷ Out of the 11,721 Suspicious Activity Reports filed by the securities and futures industries since 2003, only 16 filings failed to identify a violation amount.

Table 2.
Violation Amounts Identified in
Suspicious Activity Reports filed by
Securities and Futures Industries

Amount Range	Number of Reports	Percentage of Total Filings
No amount reported	16	0.13%
\$0	1760	13.84%
\$1<\$9,999	1972	15.50%
\$10,000<\$49,999	3841	30.20%
\$50,000<\$99,999	1130	8.88%
\$100,000<\$499,999	1724	13.55%
≥ \$500,000	1278	17.90%

⁷ In the “Advance Fee Fraud” or 4-1-9 (a section of the Nigerian penal law that prohibits this activity) schemes, victims may receive emails and letters from groups of con artists, often located in Nigeria, who claim to have access to a very large sum of money and want to use the victim’s bank account to transfer the funds. In exchange for the victim’s services, they claim they will give the recipient of the email/letter a large percentage of the funds. These schemes have a common denominator—eventually the target of the scheme will be required to pay up-front (advance) fees (licensing fees, taxes, attorney fees, transaction fees, bribes, etc.) to receive the percentage of funds promised. The con artists usually request that they be furnished with blank company letterhead and/or bank account information. In Issue 7 of *The SAR Activity Review*, pages 47-48, FinCEN requested that financial institutions not file Suspicious Activity Reports on advance fee fraud schemes unless such schemes involve a monetary loss.

Occupation Analysis

In general, securities and futures industries filers did not report an occupation for suspects. This information appears on the Suspicious Activity Report form, but it is not required to be obtained under the Customer Identification Program rule. Only about one in 15 Suspicious Activity Reports included this information. An occupation was more likely to be listed where the suspect was associated with either the filing firm or another financial services firm. In fact, suspects in this specific category (Financial Services Industry) comprised almost 7% of those filings that reported an occupation. Occupational information assists FinCEN and law enforcement in analyzing Suspicious Activity Reports if the subject's occupation is provided.

Table 3.
Top Five Occupation Types
Identified in Suspicious Activity Reports
Filed by Securities and Futures Industries

Occupational Category	Number of Reports	Percentage of Total Filings
Financial Services Industries	884	7.01%
Manager of a firm or facility	359	2.85%
Self Employed	294	2.33%
Retired	281	2.23%
Real Estate	228	1.81%

Suspicious Activity Patterns

The most common violation reported in Suspicious Activity Reports filed by securities and futures industries, not including "Other," was "Money Laundering/Structuring." Filers reporting this violation gave examples of overt efforts to launder funds through investment accounts opened for no apparent economic purpose other than to wire funds internationally. Additionally, filers identified deposit/withdrawal activity in accounts that seemed to have no other source of net change in the account balance. Generally, suspicious activity pertaining to "Check Fraud" and "Significant Wire or Other Transaction Lacking Purpose" remained stable over the last two years, but "Identity Theft" appeared to be closing in as one of the most commonly reported suspicious activities.

Only in the first quarter of 2004 was there a fundamental change in the distribution of reported violations. Closer inspection revealed an extraordinarily high number of filings reporting “Check Fraud,” “Credit/Debit Card Fraud,” and “Wire Fraud.” These categories represented the most popular methods of funding retail brokerage accounts. Increases in these categories may indicate that retail customers were:

- (1) illiquid during this period; or
- (2) deliberately failing to fund their accounts and/or settle trades.

There was also an increase in identity theft reported during the first quarter of 2004. In many of these filings, multiple suspects attempted account piracy by trying to fraudulently fund accounts through misappropriated Automated Clearing House payments. When the Automated Clearing House transfers failed, some suspects provided booster (fraudulent) checks to falsely inflate account balances. This was done with the hope that a wire transfer might be sent to another institution before any suspicious activity was detected in the new brokerage account. This peculiar distribution did not persist into the second quarter of 2004, and the percentages in each violation category except identity theft trended back to previously observed rates.

Table 4.
Frequency of Reported Suspicious Activity
In the Securities and Futures Industries

Suspicious Activity Reported	Number of Reports Filed	Percent of Total Filings
Other	4456	23.04%
Money Laundering/Structuring	3179	16.43%
Check Fraud	1850	9.56%
Significant Wire or Other Transactions Lacking Purpose	1842	9.52%
Identity Theft	1742	9.01%
Embezzlement/Theft	1346	6.96%
Wire Fraud	1289	6.66%
Suspicious Documents or ID Presented	662	3.42%
Securities Fraud	600	3.10%
Credit/Debit Card Fraud	481	2.49%
Forgery	373	1.93%
Mail Fraud	342	1.77%
Insider Trading	277	1.43%
Market Manipulation	245	1.27%
Computer Intrusion	195	1.01%
Bribery/Gratuity	82	0.42%
Wash or Other Fictitious Trading	76	0.39%
Terrorist Financing	70	0.36%
Prearranged or Other Non-Competitive Trading (Collusion)	59	0.31%
Futures Fraud	16	0.08%
No Violation Reported	162	0.84%

Straw Accounts/Account Funding Frauds

Filers continued to report account funding fraud throughout the examination period. Some of the funding frauds occurred in conjunction with identity theft and Automated Clearing House piracy, while others occurred in conjunction with straw accounts established in the names of purely fictional individuals/entities. Filers cited attempts to fund newly established accounts with counterfeit, stolen, or bad checks, or through unauthorized Automated Clearing House payments from unknowing individuals.

It appears most financial institutions were able to identify “true name fraud”⁸ or straw entities by following their Customer Identification Programs before brokerage accounts were established; however, online broker-dealers typically reported that the detection of fraud occurred after accounts were established and transactions initiated. When monitoring suspect accounts, online broker-dealers discovered that several straw accounts with the same addresses had been established. This subsequently led to the filing of multiple Suspicious Activity Reports as filers reported straw accounts associated by similar address, phone number, or name.

Losses attributed to straw accounts and true name frauds appeared to affect online brokerage firms more than traditional brokerage firms. This may be the result of limited capabilities of online brokerages to conduct adequate account due diligence when allowing online processing of applications. Unlike traditional brokerage houses with regional registered representatives familiar with regional economic conditions and the regional consumer base, online firms have no specific regional market and thus may be vulnerable from all points. As noted above, the online application process typically may not involve any verification beyond credit bureau headers,⁹ which means no official government identification is actually reviewed as a source document to verify applicant identity.

⁸ True name fraud is the primary fraudulent technique used to initiate an account takeover. The Association of Certified Fraud Examiners defines true name fraud as an “account takeover [that] involves the thief actually taking on the true name identity of legitimate consumers.” In this case, fraud against the institution is not effected through a straw identity (fictitious person of no means) but is instead effected by misappropriation of another’s true name (18 U.S.C. § 1028) (a person of means illegally placed in a position of obligation).

⁹ “Credit header data is the identifying information that accompanies consumers’ credit reports. It consists of name, name variations, address, former addresses, telephone number (even unlisted numbers if known), date of birth (usually limited to month and/or year of birth) and Social Security number. Although credit header information is generated as part of the credit reporting process, the Federal Trade Commission has determined that it is not part of the credit history and therefore is not regulated under the Fair Credit Reporting Act.” (Source: <http://www.privacyrights.org/ar/fedres.htm>)

As described in filing narratives, online broker-dealers were more likely to let customers buy/sell and conduct wire activity in new accounts without an appreciable hold or restriction period. Online broker-dealers reported more losses related to initial funding activity that eventually (10 or more days later) proved to be fraudulent.

Automated Customer Account Transfer/Automated Clearing House/Wire Piracy

Piracy in the context of Suspicious Activity Reports indicates the takeover, or attempted takeover, of an established account or transaction by an unauthorized individual. As previously noted, a number of filers reported that individuals believed to be legitimate prospects opened accounts with the intent to fund the accounts electronically. The fraudulent funding method of choice was typically an Automated Clearing House payment or an Electronic Funds Transfer (ACH/EFT) debit of a demand deposit account.¹⁰ Filers also indicated that many suspects offered several different pirated account numbers in anticipation that initial attempts to fund an account would fail. Predictably, these Automated Clearing House/Electronic Funds Transfer debits were returned for various reasons, including insufficient funds and account restrictions due to fraud.

Electronic memorandum (account journaling) was also identified as an account takeover mechanism and a source of fraudulent funding. There were at least seven Suspicious Activity Reports that indicated fraudulent funding attempts using transferring services¹¹ offered by one particular clearing processor and/or its subsidiaries. These attempts included one subject's effort to transfer securities from an account rightfully titled in his mother's name. Another was attempted by a subject opening an account for transfer; however, the transfer failed because a securities clearing processor could not match the subject's Social Security Number to that of the legitimate account holder.

¹⁰ A demand deposit account (or DDA) is an account, usually a checking account, which permits the account owner to withdraw funds from the account on demand.

¹¹ "Transferring services" refers to systems that allow customers to transfer assets from one brokerage firm and/or bank to another.

Intentional Abuse of Accounts

The most common theme reported by filers was individuals attempting to use brokerage accounts in a manner inconsistent with the stated investment objective. The predominant activity reported in this category was funding an account but allowing the money to remain idle. Since some investment accounts are not interest bearing, failure to invest assets is actually considered a loss in most cases. Therefore, lack of activity in an investment account may serve as a red flag to broker-dealers. Filers indicated that the decision to file a Suspicious Activity Report usually was made after long periods of inactivity followed by sudden liquidation activity on the account, such as check writing, debit card use at automated teller machines, and/or outbound fund transfers sent without obvious economic benefit. Reports indicating excessive outbound wire activity were common in Suspicious Activity Reports filed by the securities and futures industries. Preliminary indicators are that individuals who engage in this activity within one year of establishing a brokerage account were more likely to send funds outside of the United States.

Several filers located near the Canadian or Mexican borders reported strong suspicions that funds in idle brokerage accounts were being wired to foreign institutions in Canada and Mexico to evade taxes. In one case, a filer reported an elaborate funds transfer scheme involving a local bank's correspondent account. Apparently, a suspect attempted to trace funds released to a customer before the item had cleared; the charge-back to the brokerage account created a margin debit¹² for several thousand dollars.

12 Margin debit is "a debit in your account that is owed to the broker. The debit is secured with stocks and bonds which regulators have authorized for use as collateral. It excludes funds due which are debits resulting from purchases in a cash account." Source: www.trader-soft.com/option-trading/option-glossary/m.html.

Computer Intrusion Violations within Depository Institutions

In a world of ever-evolving technology, computer intrusion is an important topic for individuals and especially businesses such as financial institutions that manage and harbor a great deal of personal information. For the purpose of this study, computer intrusion is defined using instruction #2 from the “When to Make a Report” section on the Suspicious Activity Report instruction sheet(s):

Computer Intrusion is defined as “gaining access to a computer system of a financial institution to:

- a. Remove, steal, procure, or otherwise affect funds of the institution or the institution’s customers;
- b. Remove, steal, procure or otherwise affect critical information of the institution including customer account information; or
- c. Damage, disable or otherwise affect critical systems of the institution.”

Our goal in examining filings reporting “Computer Intrusion” was to provide a baseline of activity observed within the population of depository institutions’ Suspicious Activity Reports. The examination established a general profile of activities identified in sampled narratives as well as meaningful associations between violating activity and other frauds.

Background

The timeframe for this study was from June 19, 2000 through June 30, 2005; June 19, 2000 was the date “Computer Intrusion” appeared as a type of violation on the Suspicious Activity Report form used by depository institutions (TD F 90-22.47). The cumulative yield of all queries for this period was 10,155 Suspicious Activity Reports.

For this study, the targeted population was limited to depository institutions reporting computer intrusion. Only filings submitted by depository institutions using the Suspicious Activity Report form (TD F 90-22.47) effective June 19, 2000 and thereafter were considered. It is important to note that *The SAR Activity Review - By the Numbers, Issue 2* (June 2001) indicated that suspicious activity reporting of computer intrusions was more

than 7,000, but this figure included filings by both depository institutions and money services businesses during that examination period. While it might appear that reports of computer intrusion declined rapidly from 2003 through the first half of 2005, this would be an incorrect characterization. During the period, money services businesses became subject to a separate suspicious activity reporting requirement (effective January 1, 2002). Because there was no reporting form specifically designed to capture money services business data on the effective date, money services businesses filed reports on form TD F 90-22.47. Use of the Suspicious Activity Report by Money Services Business form (TD F 90-22.56) began in October 2002 and mandatory reporting began in February 2003, with a six-month grace period. All suspicious activity reported by money services businesses subsequent to August 2003 was filed on the Suspicious Activity Report by Money Services Business form. From January 2002 through August 2003, money services businesses could and did use form TD F 90-22.47 (now almost exclusively used by depository institutions) to report suspicious activity. Therefore, the number of suspicious activity reports citing computer intrusion as a violation filed by depository institutions during this period seems “inflated.”

Another concern regarding data in the population is that filing institutions tended to overuse the “Other” category when characterizing a violation; therefore, the “Other” category was not included. However, filers have the ability to use the “Other” category and notate a suspected activity; those responses were reviewed for activity relating to computer intrusion.

Analysis

Between June 2000 and June 2005, 3,726 Suspicious Activity Reports identifying computer intrusion were filed. Almost 70% (1,861) of those filings occurred in 2003 and 2004. The last eight quarters show an unsteady pace in 2003 followed by an extraordinary increase (up 272% from the first quarter of 2004) in the filing rate for the second quarter of 2004. The filing rate slowed during the first half of 2005 but growth is still the prevailing trend.

In summary, accelerated growth in computer intrusion filings could be seen clearly in August 2004 when the volume of Suspicious Activity Reports filed reached 1,417. The 2004 volume exceeded cumulative total filings for all previous years (1,251), and the filing volume increased more than 200% from the first quarter of 2004 to the second quarter of 2004; however, in 2005 the volume declined slightly, with only 521 filings in the first half of the year.

Suspicious Activity – Frequency of Occurrence

There were significant fluctuations between filings relating to computer intrusion in 2000 and the first quarter of 2001. A possible explanation is that this period marked the beginning of the filing requirement and therefore represents an institutional learning curve as filers became familiar with the filing requirements. Consistent with this learning curve theory is that computer intrusion filings in the first quarter of 2001 may have been categorized “Defalcation/embezzlement,” or “Misuse of Position or Self-Dealing.” The first quarter of 2001 seemed to reflect a misapplication of the “Computer Intrusion” violation to describe the use of the bank computing function to embezzle funds or to self-deal by altering accounting functions in personal employee accounts. This learning curve persisted until the first quarter of 2002, after which time the filing volume decreased.

The volume of Suspicious Activity Reports identifying “Computer Intrusion” remained light in the second quarter of 2002. However, overall, there was a shift in other types of suspicious activity reported, specifically, the “Misuse of Position or Self-Dealing” violation which exceeded the “Check Fraud” violation during this period. In prior quarters, the “Misuse of Position or Self-Dealing” was not reported as frequently. Further review identified at least one institution that reported the fraudulent negotiation of unsolicited loan checks using this category. Even though this activity did not meet the definition of computer intrusion, this institution continued to report fraudulent check negotiations as instances of computer intrusion well into 2003. Financial institutions returned to the previous mode of reporting “Misuse of Position or Self-Dealing” in the third quarter of 2002 and that mode of reporting continued through the second quarter of 2005.

A dramatic change in the population occurred in the second quarter of 2004 as overall filing volume increased and the “Identity Theft” violation type appeared on the Suspicious Activity Report form. Reports using the “Identity Theft” violation type began with 216 filings in the second quarter of 2004, possibly indicating an association between computer intrusion and identity theft. This positive association between computer intrusion and identity theft continued into the first half of 2005. The addition of “Identity Theft” to the violation type field appeared to help better define computer intrusion as a violation. This adjustment also eliminated filings related to employee misconduct and fraudulently negotiated checks as computer intrusions. The drop in filings, coupled with important changes in observed activity, signifies a pivotal development driving the filing volume in 2004.

Violation Amounts

Generally, institutional filers were most likely to indicate that violation amounts involved in each occurrence equaled zero (\$0); however, in the fourth quarter of 2003 and throughout the first two quarters of 2005, filers indicated violation amounts within the range of \$1 to \$9,999 more commonly than violation amounts equal to zero (\$0). This clearly indicates an emerging trend in actual losses reported by institutional filers. Interestingly, the timing of this trend in violation amounts corresponded to the emergence of identity theft and debit card fraud as leading violations in early 2004. Further review of these violations indicated they typically occurred in the presence of spoofing/phishing attacks.¹³ The emergence of filers reporting financial loss and the emergence of identity theft and debit card fraud may support the theory that a new pattern of vulnerability involving spoofing/phishing attacks was on the rise throughout 2004 and into 2005.

Institutions Reporting

According to the Anti-Phishing Working Group¹⁴ (APWG)--Phishing Activity Trends Report of October 2004, financial institutions have historically been the most targeted industry sector in the number of spoofing and phishing attacks.¹⁵ The report also indicated that increased suspicious activity reporting of computer intrusion was probably influenced by the number of people opting for online banking services. The phishing/spoofing attacks on institutions reported by the Anti-Phishing Working Group was compared to Suspicious Activity Reports identifying computer intrusion in order to recognize possible meaningful associations. Almost immediately, the phishing/spoofing attacks identified by the Anti-Phishing Working Group on one financial institution in particular could be associated with suspicious activity reporting patterns. The Suspicious Activity Reports filed by this institution were detailed and provided actual dates and language of the spoofed email. When compared with filing specifics reported by the Anti-Phishing Working Group archive of the alleged emails, a positive correlation between FinCEN data

13 According to the Federal Bureau of Investigation, "Spoofing or phishing frauds attempt to make Internet users believe that they are receiving email from a specific, trusted source, or that they are securely connected to a trusted web site, when that is not the case. Spoofing is generally used as a means to convince individuals to provide personal or financial information that enables the perpetrators to commit credit card/bank fraud or other forms of identity theft. Spoofing also often involves trademark and other intellectual property violations."

(<http://www.fbi.gov/pressrel/pressrel03/spoofing072103.htm>)

14 "The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types." (<http://www.antiphishing.org/index.html>)

15 Anti-Phishing Working Group, "Phishing Activity Report", http://www.antiphishing.org/APWG_Phishing_Activity_Report-Oct2004.pdf.

and Anti-Phishing Working Group open source data for at least this institution could be identified.

The strong association between the FinCEN data and Anti-Phishing Working Group open source data allowed a model of activity to be developed for this institution based on the launch of the phishing email and the time of detection. This model identified that the average filing lead time for an incident of phishing/spoofing normally exceeded 60 days. The incident of phishing/spoofing typically:

- was identified after a customer reported an account as compromised;
- exceeded 25 days from date of the phishing/spoofing email; and
- occurred within either one week before or after the first of each month (i.e., August 24 through September 7).¹⁶

While the 2004 phishing/spoofing attacks reported by the Anti-Phishing Working Group identified attacks against large banking organizations, only a few were filers of computer intrusion-related Suspicious Activity Reports. Narrative analysis revealed that only two of the large banks actively and consistently reported phishing/spoofing attacks. The other large banking organizations reported an assortment of activities which often involved employee misconduct.

Geographic Analysis

Fluctuations in state frequency of Suspicious Activity Report filings were compared to fluctuations in the Federal Deposit Insurance Corporation's "Regional Economic Conditions" report to identify possible influences. For example, the number of suspects having a reported state residency of Michigan was 89, or 8.15% (Table 5) of the target population that listed a suspect's state of residence. Michigan, however, represented only 3.53% of the overall population, according to the 2000 U.S. Census. Further review of

¹⁶ Attackers may target this period around the first of each month given the typical monthly statement cycles of depository institutions.

Michigan's Suspicious Activity Report filings revealed that one filer routinely reported employee misconduct involving bank computers as computer intrusions, while another filer (mentioned previously) inappropriately categorized fraudulently negotiated, unsolicited loan checks using email as computer intrusion.

An examination of national averages for unemployment rate, payroll employment growth rate, and personal bankruptcy filings was performed to determine if there were measurable associations between these economic indicators and Suspicious Activity Report filings reporting computer intrusion.¹⁷ The number of households participating in online banking services from 2000 to 2004, as reported by Forrester Research, was also examined. An extended review of economic activity in Michigan between the third quarter of 2003 and the second quarter of 2004 indicated that total payroll employment growth in Michigan lagged behind the U.S. national average, while personal bankruptcy filings outpaced the U.S. national average. This provided a model of activity related to unexpected increases in the number of suspects identified in Suspicious Activity Reports reviewed. At least two other states examined in the same period fit this model: Colorado, with a suspect frequency of 4.30% and a census percentage rank of 1.53%; and Alabama, with a suspect state frequency of 3.04% and a census percentage rank of 1.58%. This observation did not prove to be a causal relation, but there was strong evidence supporting a hypothesis that regional economic squeeze may have been, in part, a causal factor for the violations reported in Suspicious Activity Reports from some regions. Generally, however, the influence of economic conditions proved inconclusive for the remaining regions.

¹⁷ National averages were identified by the Federal Deposit Insurance Corporation Regional Economic Conditions (FDIC RECON) Quick Link for Analysts, <http://www2.fdic.gov/recon/index.asp>.

Table 1
Top Ten States as a
Function of Suspect State

State	Actual Reports	Percentage of Total Actual Reports
CA	114	10.44%
MI	89	8.15%
FL	79	7.23%
TX	77	7.05%
NY	67	6.14%
CO	47	4.30%
IL	45	4.12%
PA	45	4.12%
GA	43	3.94%
OH	41	3.75%

A troubling characteristic of the computer intrusion-related Suspicious Activity Reports was that there was a high number of suspects for whom locations were unknown (more than 1,800) to the financial institution. This was consistent with account compromise by unknown suspects and suggested a lack of geographic affinity between suspects and financial institutions. This finding was also consistent with the second quarter of 2004 shift to the “Identity Theft” violation as it became obvious that computer intrusion was a remote and anonymous offense.

Occupation Analysis

Occupational data reported by depository institutions on the Suspicious Activity Report form (TD F 90-22.47) was collected in two ways: (1) filers indicated a suspect’s affiliation with the filer in a pre-coded response; or (2) filers indicated a suspect’s occupation in a free-form response, which was post-coded for quality control.¹⁸ While post-coded responses were always mutually exclusive, the pre-coded responses were not and, therefore, suspects were identified by multiple codes.

¹⁸ Question #30 on the Suspicious Activity Report form asks the filer to identify the suspect’s “Relationship to Financial Institution” (i.e., A-Accountant, B-Agent, C-Appraiser, D-Attorney). Responses A-K are considered pre-coded responses, and response “L-Other” allows the filer to write in a response (post-coded).

In general, responses to the question on the Suspicious Activity Report form, “Is individual/business associated/affiliated with the reporting institution?” identified 1,466 suspects without a customer affiliation with the filing institution, while 2,132 filings identified suspects with a customer or borrower relationship with the filing institution. This finding is difficult to reconcile because associations were not mutually exclusive; for example, filing institutions regularly listed employees as both employee and customer. There were also 2,369 filings that indicated “Suspect Information Unavailable” that did not identify a suspect or an occupation.

Examination of bank personnel reported as suspects revealed that at least 15 had high-level access to bank computing infrastructures (i.e., bank network administrators). There were also occasional reports that identified the names of malicious codes (i.e., viruses,¹⁹ worms,²⁰ and Trojans²¹) introduced to bank servers. In each instance of malicious code, the infection occurred in systems deemed non-critical to bank operations, e.g., the Internet security systems, email, or servers (email and networking systems). While data corruption of non-critical systems did not meet the strict definition of computer intrusion, it may have imposed a significant burden on bank operations. Some of the malicious codes identified included:

- Lovesans worm;
- W95@mm virus;
- W32.Bugbear.B@mm virus; and
- W32.Bugbear.B.dam virus

In the case reporting the Lovesans worm, an Internet security systems server enabling web-based production was infected and quarantined; all other reports related to quarantined email attachments.

19 In computer security technology, a virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents (for a complete definition, see below). Thus, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of the virus into a program is termed infection, and the infected file (or executable code that is not part of a file) is called a host. ([en.wikipedia.org/wiki/Virus_\(computing\)](http://en.wikipedia.org/wiki/Virus_(computing)))

20 A computer worm is a self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers. ([en.wikipedia.org/wiki/Worm_\(computing\)](http://en.wikipedia.org/wiki/Worm_(computing)))

21 A Trojan is a computer program that disguises itself as a useful software application that is actually used to gain access to a computer. Trojans are named after the Trojan horse used by the rescuers of Helen of Troy. (www.tecc.com.au/tecc/guide/glossary.asp)

Narrative Analysis

Narratives of 140 Suspicious Activity Reports were reviewed and coded for 16 causal behaviors and 23 resultant behaviors. Causal targeting focused on methods compromising both bank systems and customer information files, while resultant targeting focused on the types of accounts compromised and losses occurring after compromise.

Anomalies appeared sporadically throughout the narrative sample, some previously discussed, including cases of advanced fee frauds, fraudulent negotiation of loan starter checks, employee misappropriation of customer information files prior to separation from the filing institution, and employee misconduct involving the use of bank systems to alter personal account terms. The anomalies did not meet the definition of computer intrusion and therefore were not evaluated extensively.

The narrative content exhibited a change consistent with changes in the nominal data identified in the second quarter of 2004. Before exploring these changes further, it is important to note that the current best practices for online banking require public key access to a vaulted site (sites using session cookies only), which means that the examination did not expect to encounter instances of man-in-the-middle eavesdropping. In addition, public encryption keys for most online banking services is now 128-bit encryption and the examination did not expect to encounter instances of session hijacking. In fact, the compromise of bank-hosted servers containing customer information files was not a common occurrence in the sampled narratives. Of the narratives reviewed, seven suspicious activity reports indicated a compromise to customer information files maintained on bank-hosted servers. All seven filings, in 2002 or earlier, reported no further indications that customer information “had been accessed or otherwise abused.” Targeted analysis of reported attempts to breach non-customer information file bank-hosted server(s) indicated that attacks on bank-hosted servers (e.g., Internet security systems, web, proxy)²² first appeared in the population in the second quarter of 2001 but disappeared by the third quarter of 2003.

²² Proxy is a server that manages the hypertext transfer protocol (HTTP) for the World Wide Web.

Account Types Compromised

The most commonly compromised account type was the demand deposit account,²³ with either a compromise of the principal account and the personal identification numbers or a compromise of a debit card number and the personal identification number. Filings reporting the compromise of a principal account and the personal identification numbers were more likely to report that a victim's identity was assumed by someone known to the victim, including bank personnel. Unauthorized transaction activity associated with this type of account compromise included use of the account and personal identification numbers to initiate Automated Clearing House payments through online bill payment services and/or to make check requests.

Compromise of branded debit cards to access demand deposit accounts were more likely to be associated with filings that listed a suspect as unknown. It should be noted that breaches of this nature were far more common than compromises of the principal account and personal identification number. Unauthorized transactions associated with this type of account compromise included debit card usage resulting in unauthorized charges and card clones²⁴ used to withdraw funds via automated teller machines.

The second most commonly compromised accounts were credit card lines of credit, where the credit card number was compromised. This type was reported by several unrelated financial institutions and was associated with a single event in which bank identifier codes for a large brand credit processor were compromised.

Other types of deposit, revolving and installment accounts, such as first and second mortgages, overdraft protection accounts, and one instance of a purser account, appeared in the narrative sample. Most of these occurrences were associated with bank employee misconduct, including the use of the computing function to alter balances, refund or retard fees collected, and change due dates.

23 A demand deposit account (or DDA) is an account, usually a checking account, which permits the account owner to withdraw funds from the account on demand.

24 A cloned credit or debit card is a counterfeit card created using the real customer's account number and other identifiers found on the face (and sometimes, the back) of the card. It is also referenced as "white plastic."

Methods of Account Compromise

To better explain the nature of security and how accounts can be compromised, a general review of the meaning of “hacking” and the typology associated with “hacking” is required as follows:

Overview of Hacking

In the original sense of the term, a hacker is an expert programmer. Over the years, the term “hacker” has lost its original meaning and has become a term associated with malicious programmers. The hacker’s prize is the satisfaction of cracking the defenses of another programmer while misappropriation of funds or data is the trophy of a successful hack. Each time a new product or service is rolled out with the intent to capture more broadband users, a new set of vulnerabilities awaits discovery by hackers. Ultimately, firewalls are the last defense between proprietary information and hackers. Quite possibly, every program may be cracked, which means that network administrations (banking or otherwise) are barely one step ahead of the hackers and should consider all areas of vulnerability when designing secure websites.

Types of Hacker Attack

In general, there are only two methods of attack, direct and indirect. A direct attack attempts to deliver scripts²⁵ directly to targeted devices. Even when direct attacks are initiated in stealth mode, hackers generally regard direct attacks as the riskiest because active pinging²⁶ increases chances of detection. On the other hand, an indirect attack delivers scripts to component programs (e.g., electronic mail) of the target server that will eventually become integrated into the root directories of the target device. Once these scripts are delivered, a trigger (e.g., time, logic or other devices) will drop additional malicious codes (i.e., trojans, viruses, worms) into the legitimate command scripts of a targeted device. The downloaded malicious codes can result in a wide variety of attacks and/or damage, including flooding, overflows, phishing/spoofing, denial of service, data diddling (corruption), and altered/hijacked URLs²⁷ (web defacement). For this study, if a narrative indicated a compromised server, it was assumed a direct attack

25 Scripts are computer programming code written in relatively simple programming languages. (www.c-latitude.com/glossary.asp)

26 “Ping is a basic Internet program that lets you verify that a particular Internet address exists and can accept requests. The verb ping means the act of using the ping utility or command. Ping is used diagnostically to ensure that a host computer you are trying to reach is actually operating.” (www.indrum.com/planet/glossary.htm)

27 URL is an acronym for Uniform Resource Locator, which is “a string of characters that represents the location or address of a resource on the Internet and how that resource should be accessed. World Wide Web pages are assigned a unique URL.” Source: www.iarchive.com/_library/terminology/u.htm.

on the server had occurred. Direct attacks, by definition, require that rootkits with backdoor scripting have either been installed or that there was an attempt to install these scripts.

Findings within Computer Intrusion-Related Suspicious Activity Reports

In the last eight quarters covered by the analysis, there were five filings included in the narrative sample that indicated hacking attempts on the customer information file server(s) had occurred (none were successful), and no filings indicated a third party processor had been compromised. This was in stark contrast to filings in 2000 to 2002 that indicated at least 11 hacking attempts on customer information file servers, and, as previously stated, seven probable hacks of customer information file servers. At least 22 filings indicated successful compromise of third party processors. Changes in computer intrusion activity may support financial institutions' claims that bank-hosted servers are secure.

Compromise Of Third Party Processors

As previously stated, activity observed between 2000 and 2002 was quite different from activity observed from 2003 through the second quarter of 2005. One of the most obvious differences was that third party processors were finding it difficult to secure customer information files in the period of 2000 to 2002. There were four third party processors identified in 22 Suspicious Activity Report narratives, and all four were contract hosts for online banking and/or online bill payment services for different banks. In all cases, a direct hack of database servers was identified as the probable point of compromise and in at least one high profile case, arrests and convictions followed. In at least seven narratives filed between 2000 and 2002, filers hosting critical files for non-core banking activities indicated hosting servers were compromised. In three of the seven narratives, filers indicated a suspect contacted them to demand funds in exchange for the return of critical information. At least one overseas extortionist was wired \$10,000 at the direction of the Federal Bureau of Investigation Internet Crimes Complaint Center (IC3)²⁸ task force agents. Literally thousands of accounts were compromised during these attacks.

28 Federal Bureau of Investigation: Internet Crimes Complaint Center (IC3) is the joint task force led by the FBI and the National White Collar Crime Center with the primary mission being the investigation of Internet crimes. This task force, formerly known as the Internet Fraud Complaint Center (IFCC), is a primary source for confidential leads, which are provided directly to the task force by victims of Internet frauds.

Since the fourth quarter of 2004, there were no additional reports identifying compromised third party processors. As mentioned previously, the four third-party processors that experienced a direct hack to their servers claimed to have increased servicing volumes, which may indicate the computing infrastructure for bank-contracted servicers has been strengthened.

Compromise of Customer Information Files

In contrast, the compromise of customer information files for branded credit card processors appeared only twice between 2000 and 2002, although thousands of accounts were compromised in each instance. However, card processors appeared five times in the last eight quarters of the analysis and several filings indicated that damages could not be estimated because not all unauthorized activity had been reported by legitimate customers. At least two filings indicated a direct hack of servers which occurred at a firm contracted out by a credit card processor.²⁹

‘Spoofing’ and ‘Phishing’

There were several reports of denial of service attacks, both distributed and single-source, on non-critical bank servers by spoofing the Uniform Resource Locator (URL) of the target financial institution.³⁰ To “spoof” is a hacker term that means “to forge an identity.” Spoofing has been used to describe many different types of malicious activities that involve forging an identity. For instance, in the previously mentioned reports, hackers launched a denial of service attack by initiating a Transmission Control Protocol (TCP) ping to millions of devices using the spoofed Internet Protocol address of the targeted device as a reply address.

There is another type of spoofing, however, that should be a larger cause of concern because it occurs with far more frequency than instances of direct hack attacks on bank-hosted servers in the sample. This variety of spoofing involves the creation of emails that appear to be legitimate emails from banks and/or bank regulators. These emails, through social engineering, encourage recipients to compromise their account information

²⁹ A credit card processor is “a company that performs authorization and settlement of credit card payments, usually handling several types of credit and payment cards (such as Visa, MasterCard, and American Express). If merchants wish to sell their products to cardholders, they retain the services of one or more processors who handle the credit cards that the merchant wishes to accept. When a merchant retains the services of a credit card processor, it is issued a merchant ID.”

Source: <http://www.secpay.com/glossary.html>.

³⁰ Uniform Resource Locator (URL) is the unique address, which identifies a resource on the Internet for routing purposes, such as <http://www.fincen.gov>.

through illegitimate forged Uniform Resource Locators (spoofs). This collective activity is known as “phishing,” and it was the most pervasive activity reported in the sample when a suspect was unknown to the victim. Published industry reports indicate that as many as 20 email recipients out of 1,000³¹ will respond to phishing, while other industry experts have recently argued that the ratio may be closer to 1 in 8.³²

Causal Targeting

In the period from 2000 through the first quarter of 2002, Suspicious Activity Reports were coded to identify compromised online banking or bill payment services hosted by a third party processor. This targeted analysis revealed that at least four major third party processors were compromised during this period, exposing thousands of principle account numbers and personal identification numbers of retail banking customers and branded debit and credit card customers of multiple banks to hackers. Two processors accounted for over 70% (22) of the filings. One of the compromised processors determined that one of their contractors, a demographic marketing firm, was hacked and its data misappropriated by a former employee, who subsequently conspired to provide the compromised data to others. No additional compromises of third party processors were reported after the first quarter of 2002.

Causal targeting identified three types of transactions where a customer’s response to phishing was suspected: unauthorized Automated Clearing House transfers; cloned debit card usage;³³ and unauthorized bill pay/check requests. The most common transaction was an attempted Automated Clearing House transfer of funds from demand deposit accounts to accounts in the name of straw entities. Suspects typically transferred a small sum initially, but increased to larger transfers until the Automated Clearing House requests were rejected for insufficient funds or through administrative rejections for fraud. In the narratives sampled, the Automated Clearing House transactions were the most vulnerable to detection and exception reporting due to batch processing. Unauthorized Automated Clearing House activity was often halted before significant losses could occur.

31 Various; David Jevans, Testimony in front of the U.S. Senate, http://aging.senate.gov/_files/hr120dj.pdf

Greg Keizer, “Gartner sees surge in Phishing Expeditions,” Information Week, <http://www.information-week.com/story/showArticle.jhtml?articleID=19900043>.

32 Various; Dr. Dale Pletcher, “Identity Theft: The Aftermath 2003—A comprehensive study to understand the impact of identity theft on known victims,” <http://www.idtheftcenter.org/idaftermath.pdf>; Market Wire, “28% of U.S. Adults Continue to Inaccurately Identify Phishing Email Scams,” http://www.marketwire.com/mw/release_html_b1?release_id=70388.

33 Please reference footnote 24 for the definition of cloned debit card.

Cloned debit card transactions, however, were more difficult to prevent because Automated Teller Machines provide perpetrators with immediate access to cash as a result of the automated (and many times continuous) reconciliation of Automated Teller Machine networks. Customers whose accounts were compromised through cloned debit cards usually detected the unauthorized use through account statements or failed attempts to access their accounts. Unfortunately, delayed detection enabled suspects to withdraw larger amounts without fearing interception. Cloned debit card usage was reported at automated teller machines located throughout the world, including New York City, NY; Hialeah, FL; Cosa Mesa, CA; Tucson, AZ; Bucharest, Romania; Madrid, Spain; Vilnius, Lithuania; Moscow, Russia; Kiev and Zaporizhzhya, Ukraine; and Sharjah, United Arab Emirates. There were a few remarkable patterns of activity identified, including a suspect(s) operating in the Southwest, who always used Automated Teller Machines, frequently within a few blocks of a golf course and always within a few miles from the main gate of a United States military installation. Automated Teller Machines in these stores lacked mounted cameras, but a comparison of dates and times revealed that the withdrawals from unrelated accounts literally occurred within minutes of one another.

Overview of Narrative Analysis

The narrative analysis of Suspicious Activity Reports overwhelmingly identified phishing as the most pervasive and most effective manner of account compromise. This does not mean this was the only activity reported; in fact, miscellaneous activities were reported, including cases where the filing institutions failed to establish that computer intrusion had occurred. For example, filings reported web page defacement, which was specifically excluded from the definition of computer intrusion. Of greater concern was that some filers, through a routine review of available domain names discovered forged websites that could easily be mistaken for their website. In one case, the filing bank contacted the 'whois'³⁴ to determine why he had designed his web site to look like its web site. The contact advised the bank that he had broken no laws, refused to disable the site, and threatened a civil suit if the bank contacted him again. In another case, an angry bank

³⁴ 'Whois' is a term referring to a domain name search or look-up feature for a database - typically for Top-Level Domain name registries. Information such as name availability can be found through a query or search using a 'whois' protocol (standard). Most Top-Level Domain registries maintain their own 'whois' database containing domain name contact information. (Definition obtained from <http://domain.rshweb.com/glossary.html>.)

customer engaged in a campaign of targeted spam on a bank customer support mailbox. Apparently, the customer was angry over a failed transaction, which he claimed lost him considerable amounts of money. In addition to threats and libel in the emails, the filer reported the email attack rendered the bank's exchange server useless for 24 hours.

Analyst's Conclusions

In conclusion, phishing compromise was the most prevalent activity in the last eight quarters covered by this study, while hosted third party service compromise, which was prevalent in the first eight quarters, disappeared during the last eight quarters. Nothing in the last eight quarters indicated bank-hosted servers were particularly vulnerable to hacking attempts. Evidence suggested bank customers are increasingly seeking online services, but this need to be 'connected' may expose customers to scam artists seeking account information. All large banks covered by this analysis have published online banking policies. In addition, the Federal Financial Institutions Examination Committee (FFIEC) issued a brochure that explains Internet "phishing" and steps that consumers can take to protect themselves against scams.³⁵ Most of these policies warn that emails requesting sensitive account or other personal information are never initiated by the financial institution.

35 This brochure, "Internet Pirates are Trying to Steal Your Information," was distributed to financial institutions in a format that could be used as a statement insert to educate their customers and is available on the following federal banking agencies websites: <http://www.federalreserve.gov/consumers.htm> (Board of Governors of the Federal Reserve System); <http://www.fdic.gov/consumers/consumer/fighttheft/> (Federal Deposit Insurance Corporation); <http://www.ncua.gov/Publications/brochures/IdentityTheft/PhishBrochure-Print.pdf> (National Credit Union Association); <http://www.occ.gov/consumer/phishing.htm> (Office of the Comptroller of the Currency); <http://www.ots.treas.gov/docs/4/48950.pdf> (Office of Thrift Supervision).

Section 3 - Law Enforcement Cases

This section of *The SAR Activity Review* affords law enforcement agencies the opportunity to summarize investigations where Suspicious Activity Reports and other Bank Secrecy Act information played an important role in the successful investigation and prosecution of criminal activity. Each issue includes new examples from federal, state and local law enforcement agencies. Additional law enforcement cases can be found on the FinCEN website, www.fincen.gov, under the Law Enforcement / LE Cases Supported by BSA Filings link. This site is updated periodically to include new cases of interest.

Investigations Assisted by Suspicious Activity Reports

Operation Cheque Mate

Operation Cheque Mate was initiated in June 2002, after an Immigration and Customs Enforcement source provided information about a United Kingdom-based organization defrauding United States futures and securities firms. This source led to the discovery of many Suspicious Activity Reports which assisted the investigation. The two main United Kingdom operatives utilized stolen, altered or false identification to establish an online trading relationship with United States brokerage firms (small firms were preferred targets of the organization).

As part of the scheme, a United States-based operative obtained legitimate cashier's checks issued by banks in nominal amounts. Once the checks were obtained, the organization would alter or duplicate the checks, changing the amount, pay-to-order, and serial number information. The altered values of the checks ranged from \$61,000 - \$600,000. After the cashier's checks were altered, the United States-based operatives submitted signed account applications and fraudulent checks to the targeted firm via the United States mail. Under normal circumstances, a firm would not allow the account holder to trade until the check cleared (normally a 10-day check clearing period). This organization chose smaller firms, who would waive the 10-day check-clearing period in order to entice the business of customers. With the trading account established and the fraudulent checks credited to their accounts, the United Kingdom-based organization would request trading to begin immediately.

Before the end of the 10-day period, the United Kingdom-based organization would request a wire-transfer of profits to a foreign bank account in the United Kingdom, Spain and/or Argentina. Once a check was returned or identified as counterfeit, the brokerage firm incurred losses in trading fees, as well as any losses related to trading activity.

Over 50 firms were affected by this scheme, with total losses estimated in excess of \$250,000. Without early detection and the combined and coordinated efforts of law enforcement and the private sector, losses could have exceeded \$15 million.

Operation Cheque Mate involved the combined law enforcement and regulatory efforts of the Immigration and Customs Enforcement-led New York El Dorado Task Force, Immigration and Customs Enforcement Attachés in London and Paris, London Metropolitan Police (New Scotland Yard), Interpol, the Commodity Futures Trading Commission and the Securities and Exchange Commission. Private sector cooperation included: the Securities Industry Association, the National Futures Association, and over 50 additional private sector companies and associations.

Twenty individuals have been implicated in this investigation, and thirteen individuals have been indicted on a combination of charges to include bank fraud, conspiracy, concealment and international money laundering and operating an illegal money services business. Four individuals plead guilty to a combination of the previously mentioned charges, and a fifth individual was convicted of bank fraud and conspiracy following the trial.

(Source: Immigration and Customs Enforcement)

Business Accused of Structuring

Immigration and Customs Enforcement conducted an investigation based on a number of Suspicious Activity Reports involving a licensed money services business. The owners and operators of the money services business conspired with unlicensed money remitters (couriers) to commit criminal acts. The couriers brought large sums of cash to the business that were subsequently deposited into the business's bank accounts and then wired to the Middle East.

The investigation revealed that the money services business had a very limited number of clients, yet made many millions of dollars in cash deposits within a two-year period. The money services business's owners failed to file

Currency Transaction Reports for cash deposits made by their clients and prepared fraudulent records to evade the filing requirements.

Immigration and Customs Enforcement served a number of arrest and search warrants, as well as conducted subsequent consensual searches, and seized nearly \$200,000. (Source: Immigration and Customs Enforcement)

Suspicious Activity Report Leads to Conviction of Chief Executive

A Suspicious Activity Report filed by a financial institution led to a bank fraud investigation by the Federal Bureau of Investigation and the Federal Deposit Insurance Corporation's Office of Inspector General. The Suspicious Activity Report implicated a loan secretary in the misapplication of several million dollars. The resulting investigation uncovered insider abuses reaching to the chief executive officer, who was subsequently charged and ultimately pleaded guilty to assisting customers who were close friends in evading lending limits by allowing them to receive a series of loans in the names of family members and/or business associates. The chief executive officer also protected certain customers from Federal Deposit Insurance Corporation regulatory scrutiny by misapplying funds to clear overdrafts in their business accounts. The actions of these insiders contributed to the failure of the institution. The investigation has resulted in four convictions so far, including that of the chief executive officer. (Source: Federal Bureau of Investigation)

Suspicious Activity Report Initiates Bank Failure Investigation

A Suspicious Activity Report facilitated the investigation of a large bank failure that received national attention due to its size and the related criminal actions. The subject of the investigation, a former loan officer with a bank, initiated a series of nominee loans. He funneled the proceeds of these loans into his own bank account to use to purchase another bank in a different part of the state. Once the former loan officer owned the second bank, he issued a series of nominee loans from the second bank to pay the outstanding loans from the first bank. The subject might have avoided detection had the Suspicious Activity Report not caught the attention of the Federal Bureau of Investigation. The criminal conduct ultimately resulted in the failure of the second bank. The defendant and his accomplices pleaded guilty to a number of counts, resulting in six convictions and over millions of dollars in court-ordered restitution. (Source: Federal Bureau of Investigation)

Identity Thief Receives Nearly 4 Years in Prison

A suspect used “convenience checks” issued by credit card companies to steal nearly \$1 million, travel internationally, and purchase expensive items and real estate. The suspect engaged in a scheme for five years in which he created 20 fake identities and more than nine bogus business entities for which he obtained credit cards. The suspect used Social Security Numbers, which either belonged to identity theft victims or were nonexistent.

The suspect used scores of mailboxes, mail drops and commercial mail receivers in several states to accomplish this scheme, and frequently changed addresses in order to make it more difficult for his fraud to be uncovered. Using bogus or stolen identities, the suspect obtained over 100 accounts with 25 different banks. The scheme initiated when the suspect started a business to help people with credit problems. This allowed the suspect access to reports from one of the three major private credit tracking agencies.

The suspect made payments regularly on some of the cards in order to increase the credit limit. Eventually, the suspect would “bust out” the card, maxing out the credit limit by making purchases and cashing the convenience checks before abandoning the account.

This case was initiated based on the filing of a Suspicious Activity Report and was investigated by the Internal Revenue Service-Criminal Investigation. (Source: Internal Revenue Service)

Edible Delicacies Land Man in Prison

A suspect who owned a business that imported edible delicacies was sentenced to 15 months in federal prison for undervaluing the imported Asian delicacy in documentation provided to Immigration and Customs Enforcement.

The suspect pleaded guilty to structuring financial transactions to avoid reporting requirements and four counts of failure to pay federal income taxes and smuggling goods into the United States.

The suspect’s relatives also pleaded guilty to failure to file tax returns and to structuring financial transactions to avoid reporting requirements. They were each sentenced to 2 years’ probation and one of the relatives was ordered to pay restitution.

During a 3-year period, the suspect submitted numerous false invoices that undervalued shipments of the delicacies. The suspect admitted to structuring cash deposits totaling more than \$1 million that he received from the sale of the food.

This case originated with the filing of a Suspicious Activity Report and was investigated by Internal Revenue Service-Criminal Investigation.
(Source: Internal Revenue Service)

Suspect Sentenced To Five Years in Prison and Ordered to Pay \$1 Million in Restitution

A suspect who owed the Internal Revenue Service more than \$1 million was sentenced to more than five years in prison after pleading guilty to illegally structuring financial transactions and conspiring to defraud the United States Government.

The defendant's spouse also pleaded guilty to conspiracy to impair or impede the Internal Revenue Service and was sentenced to several months in prison and three years supervised release and ordered to pay restitution.

The couple operated a service-based company and failed to pay tax on the profits. Instead, they hid their profits by transferring them to a variety of offshore bank accounts in Southeast Asia.

Two co-defendants pleaded guilty to tax evasion charges for failing to report income they received from the service-based company.

This case originated with the filing of a Suspicious Activity Report and was investigated by Internal Revenue Service-Criminal Investigation.
(Source: Internal Revenue Service)

Former Executive in Prison for Tax Evasion

A suspect was sentenced to multiple months in prison and ordered to pay more than \$1 million in back taxes owed on several million dollars in income that was never reported to the Internal Revenue Service. The income was earned from two related businesses that the suspect operated during a 4-year period.

The defendant pleaded guilty to charges of income tax evasion, failure to file a tax return, obstruction of justice and making a false statement to the Internal Revenue Service. The defendant concealed the income by having a friend cash checks that were received from the business. He also submitted numerous fictitious purchase orders to the Internal Revenue Service concerning purported business expenses.

This case originated with the filing of a Suspicious Activity Report and was investigated by Internal Revenue Service-Criminal Investigation.
(Source: Internal Revenue Service)

Attorney Sentenced in Fraud Case

An attorney was sentenced to more than four years probation based on a conviction for mail fraud and structuring of currency transactions. The attorney was also ordered to pay nearly \$3 million in restitution to the victims of the various schemes and ordered to cooperate with the Internal Revenue Service in determining the correct tax liability and filing amended tax returns.

Investors lost millions as a result of the fraud scheme. As part of the scheme, the attorney promised investors that a certain product could accurately predict movements in the stock market, making it possible for software users to receive high percentage returns on stock trades and option contracts, whether the market was rising or falling.

This case originated with the filing of a Suspicious Activity Report and was investigated by Internal Revenue Service-Criminal Investigation.
(Source: Internal Revenue Service)

Owner of Service Company Sentenced in Tax Evasion Scheme

The owner of a service company was sentenced to three years in prison and two years supervised release following a guilty plea to structuring financial transactions to evade reporting requirements. An officer of the company pleaded guilty to filing a false tax return and was sentenced to 18 months in prison and one year of supervised release.

Clients of the company were instructed to issue multiple checks in amounts under \$10,000 to the company. The owner of the company admitted that during a nearly four-year period, over 800 checks were cashed at various check cashing outlets. The structured checks amounted to approximately \$3 million.

The tax returns filed by the company showed that it received gross receipts of tens of thousands of dollars in one year when in fact the company had received gross receipts of nearly \$2 million. In a second year, the company similarly underreported gross receipts.

Most of the employees of the company were paid in cash and their wages were not reported to the Internal Revenue Service nor were required taxes reported or withheld. In one quarter, the company reported to the Internal Revenue Service that it had paid wages of several thousand dollars when in fact the company had paid wages of over several hundred thousand dollars.

This case originated with the filing of a Suspicious Activity Report and was investigated by Internal Revenue Service-Criminal Investigation.
(Source: Internal Revenue Service)

Money Laundering Scheme Transferred over \$12 Million to South American Countries

Six people were convicted and sentenced for their involvement in a \$12 million money laundering scheme. The scheme involved the wire transfers of drug proceeds to South American countries for the benefit of drug cartels.

The defendants deposited drug proceeds into more than 50 bank accounts in the name of front companies, and then transferred the funds to various countries. The defendants also wired nearly \$1 million through money transmitting businesses in amounts under \$10,000 in an attempt to avoid federal reporting requirements.

This case originated with the filing of a Suspicious Activity Report and was investigated by Internal Revenue Service-Criminal Investigation.
(Source: Internal Revenue Service)

Section 4 - Tips on SAR Form Preparation & Filing

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

As in previous issues, FinCEN has reviewed recent calls received on its Regulatory Helpline³⁶ for the most frequently asked questions about suspicious activity reporting. From January to April 2005, FinCEN responded to nearly 350 calls from industry representatives to provide suspicious activity reporting guidance. An analysis of these calls revealed the demand for additional guidance in the following four areas. Note: These questions and answers will be separately posted to FinCEN's public website at www.fincen.gov.

1. Problems with Taxpayer Identification Numbers

FinCEN received numerous inquiries regarding customers conducting transactions with fraudulent, changed, unavailable, or multiple taxpayer identification numbers, including Social Security Numbers, Employer Identification Numbers, or Individual Taxpayer Identification Numbers. As institutions seek to determine whether or not a transaction is suspicious, one factor may be a consideration of the Taxpayer Identification Number used by a customer. Institutions should use reasonable discretion to determine if problems with Taxpayer Identification Numbers are suspicious in nature or otherwise explainable and not suspicious. For example, an institution may suspect that a customer provided an incorrect Social Security Number if the Detroit Computing Center generates correspondence stating that a Currency Transaction Report filed by the institution contained a customer's name and Social Security Number that did not match. If the institution determines that a teller inadvertently transcribed numbers, its risk-based response

³⁶ The financial industry can obtain regulatory guidance and answers to specific questions by contacting FinCEN's Regulatory Helpline at (800) 949-2732, or their primary functional regulator.

would be different than if it determined that the customer made a false statement by intentionally rearranging or changing numbers in an attempt to circumvent the reporting requirement. Alternatively, an institution may have software applications or other resources that reveal the number belongs to another person, or a deceased person, in which case the motive for the transaction and the inherent nature of the transaction may be characterized more clearly as suspicious.

Institutions should note that there may be legitimate circumstances in which a person conducting a transaction would have no Taxpayer Identification Number (e.g., some foreign customers of the bank), or a changed identification number (e.g., some victims of identity theft, or a sole proprietorship that has become incorporated).³⁷ Institutions should consider all of the available facts and circumstances surrounding such transactions when deciding whether or not it is suspicious.

2. Suspicious Activity at a Location Other than the Institution

A second question frequently received on the Helpline was how to complete a Suspicious Activity Report when the suspicious activity occurred at a location other than the financial institution or any of its branches. By requiring the reporting of transactions “conducted or attempted by, at, or through” an institution,³⁸ FinCEN recognizes that reportable activity does not necessarily happen at an institution’s physical location. For example, a bank debit or credit card may be stolen and then used at retail locations to purchase goods or services, but never used at the institution. Such transactions would correctly be characterized as “conducted through” the bank, and assuming appropriate thresholds were met, would require reporting.

³⁷ When a sole proprietorship incorporates, the customer’s Taxpayer Identification Number may appear to have changed, but technically has not. Most likely, the customer will retain his or her Social Security Number, and the now incorporated business will be a separate person as defined by 31 C.F.R. § 103.11(z), with a separate Employer Identification Number.

³⁸ Emphasis added. See 31 C.F.R. § 103.17(a)(2) (suspicious activity reporting regulation applicable to futures commission merchants and introducing brokers in commodities), 31 C.F.R. § 103.18(a)(2) (applicable to banks), 31 C.F.R. § 103.19(a)(2) (applicable to brokers or dealers in securities), 31 C.F.R. § 103.20(a)(2) (applicable to money services businesses), and 31 C.F.R. § 103.21(a)(2) (applicable to casinos). See also 68 F.R. 2716 (proposed suspicious activity reporting regulation for mutual funds) and 67 F.R. 64067 (proposed suspicious activity reporting regulation for insurance companies). The applicable Suspicious Activity Report regulations for each Federal Banking Agency are found at: 12 C.F.R. §21.11 (Office of the Comptroller of the Currency); 12 C.F.R. §208.62, 12 C.F.R. 211.5(k), 12 C.F.R. §211.24(f), and 12 C.F.R. §225.4(f) (Board of Governors of the Federal Reserve System); 12 C.F.R. Part 353 (Federal Deposit Insurance Corporation); 12 C.F.R. §563.180 (Office of Thrift Supervision); and 12 C.F.R. §748.1(c) (National Credit Union Administration).

When suspicious activity occurs at a location other than the institution, the filer should not put the actual location of the activity in the Suspicious Activity Report fields normally used to indicate where activity occurred.³⁹ Instead, because these fields often are used by law enforcement to determine where supporting documentation is maintained, an institution should list the location of its supporting documentation and records as the address in this field. In the Suspicious Activity Report narrative, the institution should indicate that this address is not the location of the activity, but rather where the records are being kept. Any available information about the actual location of the suspicious activity, including (for the example above) the names of the retail businesses, addresses, and contact information, should also be included in the narrative. The Suspicious Activity Report should be completed in this manner for any type of reportable suspicious activity occurring somewhere other than the financial institution. For all other transactions that occurred at the financial institution, normal filing procedures should be followed.

3. Suspicious Activity without a Loss to the Institution

A third frequently asked question involved Suspicious Activity Report filing implications when an institution discovered suspicious activity without suffering a financial loss. FinCEN reminds institutions that although the Suspicious Activity Report form has a field to indicate the amount of loss (if applicable), whether an institution suffers a loss is irrelevant to the determination of whether or not suspicious activity has occurred. For example, when cash deposits exceeding applicable thresholds are structured to avoid reporting requirements, the institution most likely will not suffer a loss, but it is required nonetheless to report such activity.⁴⁰

39 For TD F 90-22.47 (Suspicious Activity Report), box 9; for TD F 90-22.56 (Suspicious Activity Report-Money Services Business), Part III; for FinCEN Form 102 (Suspicious Activity Report by a Casino), Part IV; for FinCEN Form 101 (Suspicious Activity Report by the Securities and Futures Industries), boxes 36-41. Although all Suspicious Activity Report forms are listed here, FinCEN believes that suspicious transactions involving certain financial products offered by some institutions may not be conducive to suspicious activity at a location other than the institution offering them. Accordingly, reporting the location of suspicious activity when that activity does not occur at a financial institution may be more difficult on some Suspicious Activity Report forms than others.

40 See 31 U.S.C. § 5318(g)(1), 31 U.S.C. § 5324, 31 C.F.R. § 103.17(a)(2)(ii), 31 C.F.R. § 103.18(a)(2)(ii), 31 C.F.R. § 103.19(a)(2)(ii), 31 C.F.R. § 103.20(a)(2)(ii), 31 C.F.R. § 103.21(a)(2)(ii).

4. Insignificant Suspicious Activity Report Filing Errors

The final frequently asked question addressed in this article is whether institutions are required to correct previously filed Suspicious Activity Reports if they discover “insignificant” or “inconsequential” errors, particularly when they feel that the corrected data would be of little or no use to law enforcement. Institutions are reminded of their responsibility to make complete and accurate reports, and that any deficiency that in any way detracts from the completeness or accuracy of those reports must be amended. FinCEN further reminds institutions that information of apparent insignificance to a filer who has observed only a small part of a larger pattern of suspicious activity may be valuable to law enforcement personnel seeking a greater awareness of the entire pattern of activity. Financial institutions must file complete and accurate reports, and must correct any error they detect in accordance with the directions on the Suspicious Activity Report form.⁴¹

⁴¹ When correcting an error on a previously filed report, mark box 1 (“corrects prior report”) and follow the directions to make the necessary changes. Whenever a corrected report is filed, the institution should explain the changes in the report narrative.

Section 5 - Issues & Guidance⁴²

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

Providing Suspicious Activity Reports to Appropriate Law Enforcement

The information FinCEN collects through reporting by financial institutions is highly valuable in combating terrorism and investigating money laundering and other financial crime.⁴³ FinCEN processes and analyzes the data collected under the Bank Secrecy Act, and in accordance with applicable legal authority, makes the data available to law enforcement agencies and regulatory agencies to support their investigations and examinations. FinCEN's regulations require financial institutions to disclose all documentation supporting the filing of a Suspicious Activity Report in response to requests by FinCEN or appropriate law enforcement and regulatory agencies, including self-regulatory organizations if applicable. Such disclosures do not undermine the safe harbor provisions applicable to voluntary and mandatory suspicious activity reporting by financial institutions on disclosure of Suspicious Activity Reports.

The Bank Secrecy Act and FinCEN's regulations prohibit a financial institution that has filed a Suspicious Activity Report from notifying any person involved in the transaction that the Suspicious Activity Report has been filed.⁴⁴ Financial institutions, however, must provide such documentation to appropriate law enforcement and regulatory agencies upon request. Financial institutions should take special care to verify that a requestor of information

⁴² This guidance also will be posted under "BSA Guidance" on FinCEN's public website, www.fincen.gov.

⁴³ See 31 U.S.C. § 5311; see also 12 U.S.C. § 1951.

⁴⁴ 31 U.S.C. § 5318(g)(2)(A)(i); 31 C.F.R. § 103.17(e); 31 C.F.R. § 103.18(e); 31 C.F.R. § 103.19(e); 31 C.F.R. § 103.20(d); and 31 C.F.R. § 103.21(e).

is, in fact, a representative of FinCEN or an appropriate law enforcement or regulatory agency. Procedures for such verification should be incorporated into the financial institution's anti-money laundering compliance program or other appropriate statements of policies and procedures.

Examples of Appropriate Law Enforcement Agencies

As discussed, financial institutions are required to disclose documentation supporting the filing of a Suspicious Activity Report to an appropriate federal, state or local law enforcement agency upon request. In addition, financial institutions may share a Suspicious Activity Report, or the information contained therein, with an appropriate federal, state, or local law enforcement agency. Generally, an "appropriate law enforcement agency" is any agency that has jurisdiction under federal or state law to investigate or prosecute any person or entity involved in the transaction reported on the Suspicious Activity Report.

Examples of agencies to which a Suspicious Activity Report or the information contained therein could be provided include: the criminal investigative services of the armed forces; the Bureau of Alcohol, Tobacco, and Firearms; an attorney general, district attorney, or state's attorney at the state or local level; the Drug Enforcement Administration; the Federal Bureau of Investigation; the Internal Revenue Service or tax enforcement agencies at the state level; the Office of Foreign Assets Control; a state or local police department; a United States Attorney's Office; Immigration and Customs Enforcement; the U.S. Postal Inspection Service; and the U.S. Secret Service.

To further illustrate: financial institutions could provide Suspicious Activity Reports and any information and documents underlying them to, for example, a United States Attorney's office prosecuting an organized crime figure for money laundering; a Federal Bureau of Investigation Special Agent investigating a human trafficking ring or a Drug Enforcement Administration Special Agent investigating a suspected drug dealer; a county sheriff's office, a district attorney, or a state police department investigating or prosecuting violations of state income or sales tax law; a city police department exploring the financial aspects of a homicide investigation; and a state attorney general investigating violations of state securities laws.

Appropriate Regulatory/Supervisory Agencies

As discussed, financial institutions are required to disclose documentation supporting the filing of a Suspicious Activity Report to an appropriate federal or state regulatory/supervisory agency upon request. In addition, financial institutions may share a Suspicious Activity Report, or the information contained therein, with an appropriate federal or state regulatory/supervisory agency. Whether a supervisory agency is an appropriate requestor generally depends on whether the agency has the authority under federal and state law to examine the financial institution receiving the request for Bank Secrecy Act compliance. In the case of a depository institution, the applicable regulation specifies that federal and state bank supervisory agencies are appropriate requesters.

In the securities and futures industries, FinCEN regulations additionally permit disclosure of Suspicious Activity Reports to the New York Stock Exchange, the National Association of Securities Dealers, and the National Futures Association, as self-regulatory organizations authorized by the Securities and Exchange Commission or the Commodity Futures Trading Commission to examine financial institutions for compliance with FinCEN's regulations.⁴⁵

Subpoenas and Other Requests for Suspicious Activity Reports

FinCEN's regulations also contain specific provisions for when a financial institution receives a subpoena for a Suspicious Activity Report.⁴⁶ If a financial institution is served with any subpoena requiring disclosure of the fact that a Suspicious Activity Report has been filed or of the Report itself, except to the extent that the subpoena is submitted by an appropriate law enforcement or supervisory agency, the financial institution should neither confirm nor deny the existence of the Suspicious Activity Report. The financial institution should immediately notify the Office of Chief Counsel at FinCEN at (703) 905-3590, as well as the financial institution's federal functional regulator under that regulator's parallel requirement, if any.

⁴⁵ See 31 C.F.R. § 103.17(g) (examination and enforcement for futures commissions merchants and introducing brokers in commodities) and 31 C.F.R. § 103.19(g) (examination and enforcement for brokers or dealers in securities).

⁴⁶ See 31 C.F.R. § 103.17(e) (for subpoenas received by futures commissions merchants and introducing brokers in commodities); 31 C.F.R. § 103.18(e) (received by banks); 31 C.F.R. § 103.19(e) (received by brokers or dealers in securities); 31 C.F.R. § 103.20(d) (received by money services businesses); and 31 C.F.R. § 103.21(e) (received by casinos).

Availability of Regulatory Helpline

If a financial institution is unsure whether a particular law enforcement or supervisory agency is an appropriate requestor, the financial institution should call FinCEN's Regulatory Helpline at (800) 949-2732 for clarification.

Section 6 - Industry Forum

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into some aspect of compliance management or fraud prevention that presents their view of how they implement the Bank Secrecy Act (BSA) within their institution. Although the Industry Forum Section provides an opportunity for the industry to share its views, the information provided may not represent the official position of the United States Government.

USA PATRIOT Act's Full Weight Placed on Securities Firms

By: Alan E. Sorcher, representing the Securities Industry Association

The attacks of September 11th were a direct hit on the heart of New York's financial district and inflicted a terrible toll on the securities industry. Many innocent lives were lost and operations were thrown into disarray. In the almost four years since then, markets have returned to normal and financial institutions have undertaken many operational and system changes to conduct business in a post-September 11th world.

The USA PATRIOT Act, enacted in the weeks after September 11th, has had a major impact on the securities industry and all financial institutions. The legislation imposes its full array of anti-money laundering requirements on broker-dealers.

The USA PATRIOT Act's provisions include requirements that broker-dealers establish and maintain formal anti-money laundering compliance programs, monitor for and report suspicious activity, identify and verify new customers, maintain certain records for "correspondent accounts" with foreign banks, conduct special due diligence for foreign correspondent and private banking accounts, and not open or maintain correspondent accounts for foreign shell banks.

This article will summarize the significant provisions of the suspicious activity-reporting rule for securities firms and make some basic recommendations designed to help firms improve their overall anti-money laundering compliance efforts.

A. Suspicious Activity Report-

Suspicious activity reporting is an important part of a firm's anti-money laundering program. The suspicious activity reporting rule for broker-dealers was issued on July 1, 2002 by FinCEN under Section 356 of the USA PATRIOT Act. The rule, which took effect on January 1, 2003, applies to any broker or dealer located in the United States and to those firms registered as broker-dealers simply to permit the sale of variable annuities. The rule also applies to the activities of futures commission merchants registered as broker-dealers that involve securities products over which the Securities and Exchange Commission or any federal agency other than the Commodity Futures Trading Commission has jurisdiction.

Reportable Transactions

The broker-dealer suspicious activity reporting rule, in general, requires the reporting to FinCEN of any "suspicious transaction relevant to a possible violation of law or regulation" of at least \$5,000 in funds or other assets. Specifically, a broker-dealer must report a transaction (of at least \$5,000) if it is conducted or attempted by, at, or through the broker-dealer, and the broker-dealer knows, suspects, or has reason to suspect that the transaction (or pattern of transactions): 1) involves funds derived from illegal activity, or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity; 2) is designed, whether through structuring or other means, to evade the requirements of the Bank Secrecy Act; 3) has no business or apparent lawful purpose, or is not the sort in which the particular customer would be expected to engage, and the broker-dealer knows of no reasonable explanation after examining the available facts; or 4) involves use of the broker-dealer to facilitate criminal activity. The reporting requirements apply even to transactions that do not involve currency.

Firms are not required to review every transaction that exceeds \$5,000. Instead, firms are expected to follow a risk-based approach in monitoring for suspicious activity and to report suspicious transactions detected over \$5,000. The rule states that firms should "evaluate customer activity and relationships for money laundering risks and design a suspicious transaction monitoring program that is appropriate . . . in light of such risks." Firms must report suspicious activity even if the funds are legally derived if there is

a suspicion that the transaction is being conducted to further illegal activities, such as the funding of terrorist activity. FinCEN also encourages firms to report suspicious transactions even if they are less than \$5,000.

Exceptions to Filing

The rule includes two categories of transactions for which Suspicious Activity Reports do not have to be filed. First, violations of the federal securities laws or Self-Regulatory Organization rules committed by a broker-dealer or any of its associated persons that are otherwise required to be reported do not have to be reported on a Suspicious Activity Report as long as such violation is appropriately reported to the Securities and Exchange Commission or Self-Regulatory Organizations. The broker-dealer may be required to demonstrate that it has relied on this exception, and must maintain supporting documentation. This narrow exception from reporting does not apply, however, to violations of the securities laws or self-regulatory organization rules that require broker-dealers and government securities broker-dealers to comply with Bank Secrecy Act rules. Second, a broker-dealer is not required to file a Suspicious Activity Report for a robbery or burglary committed or attempted of the broker-dealer that is reported to appropriate law enforcement authorities, or for lost, stolen, missing or counterfeit securities that are reported in accordance with existing Securities and Exchange Commission rules.

Information Sharing by Introducing and Clearing Brokers

The suspicious activity reporting rule allows introducing and clearing firms to share information in order to determine whether a Suspicious Activity Report needs to be filed. The rule provides that the obligation to identify and report a suspicious transaction “rests with each broker-dealer involved in the transaction,” but that only one Suspicious Activity Report must be filed, provided that such report includes all of the relevant information. This permits introducing and clearing firms to communicate about a transaction and determine whether a Suspicious Activity Report needs to be filed. In this situation involving a joint filing, the firm filing the Suspicious Activity Report may provide a copy to the other firm involved in the transaction. Broker-dealers should bear in mind, however, that communication between two broker-dealers about the filing of a Suspicious Activity Report (or the sharing of a Suspicious Activity Report) may be inappropriate when a broker-dealer suspects that it is required to report the other broker-dealer (or one of its employees) as the subject of a Suspicious Activity Report.

Filing the Suspicious Activity Report

Suspicious Activity Reports are to be filed on a form “Suspicious Activity Report by the Securities and Futures Industries” with FinCEN. The report must be filed within 30 days of the broker-dealer becoming aware of facts that may constitute a basis for filing. If a firm is unable to identify a suspect, filing may be delayed for an additional 30 days in order to identify a suspect. In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, the broker-dealer must immediately notify the appropriate law enforcement agency by telephone in addition to filing a Suspicious Activity Report. The supporting documentation should not be filed with the Suspicious Activity Report form.

The rule requires firms to maintain copies of all Suspicious Activity Reports filed and the original supporting documentation for five years from the date of the filing. In addition, the supporting documentation must be made available to law enforcement or authorized regulatory agencies and the Self-Regulatory Organizations for purposes of examining for compliance with the rule.

Restrictions on Disclosing the Suspicious Activity Report

The suspicious activity reporting rule incorporates the statutory terms of 31 U.S.C. § 5318 (g)(2), which prohibits a firm that files a Suspicious Activity Report from notifying any person involved in the reported transaction that a report has been made. This prohibition does not apply to requests from FinCEN, the Securities and Exchange Commission, Self-Regulatory Organizations, or other law enforcement or regulatory agencies. A firm otherwise subpoenaed or requested to disclose a Suspicious Activity Report or the information contained therein should decline to produce such information and notify FinCEN.

Firms are protected from liability for reporting suspicious activity (even when voluntarily reporting for transactions under \$5,000) and for failing to disclose such reporting. Thus, a broker-dealer and any of its directors, officers, employees or agents that report suspicious activity pursuant to the rule will not be held liable to any person for any disclosure contained in, or for failure to disclose the fact of, such report. This protection is also applied in arbitration proceedings.

B. Recommendations to Improve Anti-Money Laundering Efforts

Suspicious Activity Monitoring Should Fit Your Firm

Because financial institutions must now sort through the thousands upon thousands of transactions that occur each day, a firm's system for monitoring and reporting suspicious activity should be risk-based, and determined by factors such as the firm's size, nature of its business, and kinds and location of its customers. For comprehensive (but not exhaustive) lists of the "red flags" of potential money laundering activity, firms should review Securities Industry Association *Suggested Practices for Detering Money Laundering Activity*⁴⁷ and the National Association of Securities Dealers *Notice to Members 02-21*.⁴⁸

Information Sharing May Help Fact Gathering

To help in the identification of suspicious activity, firms should consider taking advantage of the USA PATRIOT Act's procedures for voluntary information sharing between or among financial institutions under Section 314(b). This can be a particularly useful provision given that customers often have accounts at multiple financial institutions and that money laundering often involves the movement of monies between firms. The sharing of information must be for the purpose of identifying and reporting activities that may involve money laundering or terrorist activity. Remember that a financial institution that intends to share information and avail itself of the safe harbor for financial institutions that share information under Section 314(b) must file a notice with FinCEN using the form set forth in the rule, and must submit a new form to FinCEN each year. A financial institution, prior to sharing information with another financial institution under this rule, must take reasonable steps to verify that its counterpart has filed its own notice with FinCEN. A financial institution that does not intend to share information under the rule, however, is not required to notify FinCEN.

47 <http://www.sia.com/moneyLaundering/pdf/AMLguidance.pdf>

48 http://www.nasd.com/web/groups/rules_regs/documents/notice_to_members/nasdw_003704.pdf

Anti-Money Laundering Programs Should Encompass All Bank Secrecy Act Rules

An anti-money laundering program should also take account of all of the other relevant Bank Secrecy Act requirements (as amended by the USA PATRIOT Act) in addition to suspicious activity reporting. As part of its anti-money laundering program, a firm should have procedures to search its records in response to any request received from FinCEN under Section 314(a). Although not under the Bank Secrecy Act, broker-dealers should also have policies and procedures – whether part of their anti-money laundering program or not – to comply with the regulations of the Office of Foreign Assets Control, which administers and enforces U.S. economic and trade sanctions against targeted foreign countries, terrorism sponsoring organizations and international narcotics traffickers.

Invest in Training

An anti-money laundering program is only as good as the individuals responsible for implementation. Effective compliance relies on the judgments of those individuals, who all too often are required to make snap decisions based on imperfect information. Thus, firms should devote necessary resources to training their staff involved in anti-money laundering compliance, and should not view training as a “one-time shot.” Firms should assess which of its employees need to receive additional training, and the required frequency and level of training should be determined by the employee’s responsibilities. Moreover, current employees may require training on new requirements or refresher training. Clearly, investments made in training are well spent.

For a program to be truly effective, firm management must be willing to fully support the program, dedicate the necessary resources, and create a culture committed to adherence to the firm’s policies.

Audit is an Invaluable Tool

Firms must have their anti-money laundering programs audited on at least an annual basis by either external or internal auditors. Firms should carefully review the audit report and ensure that necessary action is taken on any of its recommendations. Whether through the anti-money laundering audit or in some other fashion, a firm should periodically evaluate its anti-money laundering program to ensure that it keeps up with changes in the firm’s business, customer base, marketplace, and technology.

C. Conclusion

The battle against money laundering and terrorist financing presents enormous challenges. Advances in technology and the widespread use of the Internet have created opportunities for those who wish to harm us no matter where they are located. Notwithstanding the achievements of the public and private sectors in implementing the USA PATRIOT Act, more can be done. While the USA PATRIOT Act provides significant tools to combat illicit activity, to be successful law enforcement and industry must continue to coordinate their efforts, and work hand-in-hand.



Section 7 - Feedback Form

Financial Crimes Enforcement Network Department of the Treasury

*Your feedback is important and will assist us in planning future issues of **The SAR Activity Review**. Please take the time to complete this form. Thank you for your cooperation.*

A. Please identify your type of financial institution.

Depository Institution:

- Bank or Bank Holding Company
- Savings Association
- Credit Union
- Edge & Agreement Corporation
- Foreign Bank with U.S. Branches or Agencies

Securities and Futures Industry:

- Securities Broker/Dealer
- Futures Commission Merchant
- Introducing Broker in Commodities
- Mutual Fund Operator

Money Services Business:

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

Casino or Card Club

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

Other (please identify): _____

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

1=Not Useful, 5=Very Useful

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

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

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

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

Yes

No

F. What new TOPICS, TRENDS, or PATTERNS in suspicious activity would you like to see addressed in the next edition of *The SAR Activity Review – Trends, Tips & Issues*? Please be specific - Examples might include: in a particular geographic area; concerning a certain type of transaction or instrument; other hot topics, etc.

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

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

October 2000 June 2001 October 2001 August 2002

February 2003 November 2003 August 2004 April 2005

Please fax Feedback Forms to:

**Financial Crimes Enforcement Network (FinCEN)
(703) 905-3698**

Appendix

Index of Topics from previous issues of The SAR Activity Review

Topic	Issue	Page	Hyperlink Address to SAR Activity Review Issue
Automated Teller Machine (ATM) Commonly Filed Violations	7	23	http://www.fincen.gov/sarreviewissue7.pdf
Automobile Retail Industry: SAR Analysis – Indications of Suspicious Activity	5	27	http://www.fincen.gov/sarreviewissue5.pdf
Boat/Yacht Retail Industry: SAR Analysis – Indications of Suspicious Activity	5	31	http://www.fincen.gov/sarreviewissue5.pdf
Broker-Dealer SARs – The First Year	7	20	http://www.fincen.gov/sarreviewissue7.pdf
Casino and Card Club Industries – Suspicious Activity Report Filings	8	19	http://www.fincen.gov/sarreviewissue8.pdf
Computer Intrusion	3	15	http://www.fincen.gov/sarreviewissue3.pdf
Computer Intrusion Violations within Depository Institutions	9	15	http://www.fincen.gov/sarreviewissue9.pdf
Consumer Loan Fraud	7	27	http://www.fincen.gov/sarreviewissue7.pdf
Correspondent Accounts and Shell Company Activity	2	18	http://www.fincen.gov/sarreview2issue4web.pdf
Coupon Redemption Fraud	6	14	http://www.fincen.gov/sarreviewissue6.pdf
Credit/Debit Cards: Suspicious Activity	4	29	http://www.fincen.gov/sarreview082002.pdf
Director’s Forum: Issue 8	8	3	http://www.fincen.gov/sarreviewissue8.pdf
Director’s Forum: Issue 9	9	3	http://www.fincen.gov/sarreviewissue9.pdf
Egmont Group- Strategic Analysis Initiative	2	24	http://www.fincen.gov/sarreview2issue4web.pdf
FATF Typologies Exercise	2	23	http://www.fincen.gov/sarreview2issue4web.pdf
Food Stamp Fraud Using Electronic Benefit Transfer (EBT) Cards	7	9	http://www.fincen.gov/sarreviewissue7.pdf
Global Use of SARs	2	24	http://www.fincen.gov/sarreview2issue4web.pdf
Index of Topics from Previous SAR Activity Review Issues	6	85	http://www.fincen.gov/sarreviewissue6.pdf
Identity Theft	2	14	http://www.fincen.gov/sarreview2issue4web.pdf
Identity Theft – Update	3	24	http://www.fincen.gov/sarreviewissue3.pdf
Increased SAR Reporting Involving Mexico	1	12	http://www.fincen.gov/sarreviewforweb.pdf
Indicators of Misuse of Informal Value Transfer Systems	5	18	http://www.fincen.gov/sarreviewissue5.pdf
Industry Forum: Check Fraud Loss Report	5	69	http://www.fincen.gov/sarreviewissue5.pdf
Industry Forum: Check Fraud Loss Report	1	29	http://www.fincen.gov/sarreviewforweb.pdf

Industry Forum: FinCEN & Regulatory Agencies Respond to Industry Forum Comments	7	51	http://www.fincen.gov/sarreviewissue7.pdf
Industry Forum: Number of SAR Filings Should Not Determine Adequate SAR Program	7	49	http://www.fincen.gov/sarreviewissue7.pdf
Industry Forum: Questions and Answers on MSBs	2	38	http://www.fincen.gov/sarreview2issue4web.pdf
Industry Forum: Some Tips for Auditing the Suspicious Activity Reporting Program	6	71	http://www.fincen.gov/sarreviewissue6.pdf
Industry Forum: Recommended Security Procedures for Protecting Customer Information	3	45	http://www.fincen.gov/sarreviewissue3.pdf
Industry Forum: Safe Harbor Protection for Employment References	4	53	http://www.fincen.gov/sarreview082002.pdf
Industry Forum: An Overview of Suspicious Activity Report Training Elements in 2005	8	43	http://www.fincen.gov/sarreviewissue8.pdf
Industry Forum: USA PATRIOT Act’s Full Weight Placed on Securities Firms	9	47	http://www.fincen.gov/sarreviewissue9.pdf
Issues and Guidance: Advanced Fee Schemes	4	49	http://www.fincen.gov/sarreview082002.pdf
Issues and Guidance: Applicability of Safe Harbor	3	44	http://www.fincen.gov/sarreviewissue3.pdf
Issues and Guidance: Applicability of Safe Harbor	2	37	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: BSA Guidance – IRS Computing Center / FinCEN Help Line & Website	6	65	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Cessation of Relationship/Closure of Account	1	27	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: Disclosure of SAR Documentation	2	36	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Disclosure of SARs and Underlying Suspicious Activity	1	28	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: FAQs from FinCEN Help Line – 314a Process	6	59	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: FAQs from FinCEN Help Line – MSB SAR Reporting Questions	6	61	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Filing SARs on Activity Outside the United States	2	35	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Filing SARs on Continuing Activity after Law Enforcement Contact	2	35	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Filing SARs on OFAC List or 314(a) Matches	6	64	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Financial Institutions Hotline	3	43	http://www.fincen.gov/sarreviewissue3.pdf
Issues and Guidance: Florida Appeal Court Decision re: SAR production	6	65	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Guidance as to What to do When Asked for Production of SARs	7	45	http://www.fincen.gov/sarreviewissue7.pdf
Issues and Guidance: National Security Letters and Suspicious Activity Reporting	8	35	http://www.fincen.gov/sarreviewissue8.pdf
Issues and Guidance: Office of Foreign Assets Control (OFAC)	4	49	http://www.fincen.gov/sarreview082002.pdf
Issues and Guidance: Office of Foreign Assets Control’s List of Specially Designated Nationals and Blocked Persons- Revised Guidance on filing Suspicious Activity Reports	8	38	http://www.fincen.gov/sarreviewissue8.pdf
Issues and Guidance: PATRIOT Act Communications System	5	65	http://www.fincen.gov/sarreviewissue5.pdf
Issues and Guidance: Prohibition on Notification	2	36	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Providing Suspicious Activity Reports to Appropriate Law Enforcement	9	43	http://www.fincen.gov/sarreviewissue9.pdf
Issues and Guidance: Repeated SAR Filings on Same Activity	1	27	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: SAR Disclosure as part of Civil Litigation	4	50	http://www.fincen.gov/sarreview082002.pdf

Issues and Guidance: SAR Guidelines for Reporting Advance Fee Schemes	7	47	http://www.fincen.gov/sarreviewissue7.pdf
Issues and Guidance: SAR Rulings: SAR Disclosure	5	66	http://www.fincen.gov/sarreviewissue5.pdf
Issues and Guidance: Suspicious Activity Involving the Iraqi Dinar	8	41	http://www.fincen.gov/sarreviewissue8.pdf
Issues and Guidance: Timing for SAR filings	1	27	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: USA PATRIOT Act: 314(a) Information Requests	5	66	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: 314(a) Results Enhance Material Support for Terrorism Case	7	30	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Attorney and Three Accomplices Convicted in Multi-Million Dollar Real Estate Fraud	7	35	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Attorney Sentenced in Fraud Case	9	36	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Black Market Peso Exchange	2	28	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Bank Failure Investigation	9	33	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Bank President Guilty in Loan Fraud	7	34	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Bankruptcy Bust-out Scheme	6	42	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Bankruptcy Fraud Involving Family Members	6	41	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: BSA Data Leads to \$18 Million Seizure	7	31	http://www.fincen.gov/sarreview2issue9.pdf
Law Enforcement Case: Business Accused of Structuring	9	32	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Charity Evades Reporting Requirement	8	26	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Check Cashing Business	3	34	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Check Kiting Suspect	2	29	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Cocaine Trafficker	2	30	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Computer Chip Theft Ring	3	33	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Conviction of Pharmacist	5	54	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Conviction of Chief Executive	9	33	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Counterfeit Check Fraud	1	17	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Credit Card Theft	2	30	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Criminal Organization – Baby Formula	1	18	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Customs Fraud	1	17	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Drug Money Laundering	1	22	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Drug Trafficker Forfeits Structured Cash	7	35	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Drug Trafficking and Money Laundering	2	29	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Edible Delicacies Land Man in Prison	9	34	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Embargo Investigation	2	28	http://www.fincen.gov/sarreview2issue4web.pdf

Law Enforcement Case: Embezzlement	1	16	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Extortion and Title 31	3	29	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Food Bank Theft	1	19	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Forgery of U.S. Treasury Checks	6	44	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Former Banker Sentenced for Avoiding IRS Reporting	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Former Executive in Prison for Tax Evasion	9	35	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Hawala Investigation	6	38	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Hawala Operation	8	26	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Identity Thief Receives Nearly 4 Years in Prison	9	34	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Illegal Casa de Cambio	3	34	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Illegal Money Transfers to Iran	5	51	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Illegal Money Transfers to Iraq	4	35	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Importance of SAR Reporting to Law Enforcement Investigations	3	37	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Individual Operating as Unlicensed Money Transmitter	7	30	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Insider Fraud Contributes to Bank Failure	8	28	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Insurance Executive Embezzled from Local Government's Self-Insured Health Fund	7	36	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Internal Fraud at Local Bank	5	54	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: International Money Laundering Case	4	36	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Investment Firm CEO	5	53	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Investment Fraud Scheme	6	43	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Investment Fraud Scheme	1	16	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Investment Scam	3	30	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Marijuana Farm Owner Sentenced	8	27	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Medicaid Fraud	1	22	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Metal Traders Charged in International Bank Fraud Scheme	4	36	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Methamphetamine Production Ring	3	31	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Money Laundering and Pyramid Scheme	8	28	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Money Laundering by RV Dealer	3	30	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Money Laundering in Maryland	4	39	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Money Laundering involving Insurance Industry	5	53	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Money Laundering involving Iraq	6	39	http://www.fincen.gov/sarreviewissue6.pdf

Law Enforcement Case: Money Laundering of Marijuana Sales Proceeds	6	44	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Money Laundering Scheme Transferred over \$12 Million to South American countries	9	37	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Money Remitter Sending Money to Iraq	5	52	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Money Remitting Business Laundering Drug Proceeds	8	28	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Nigerian Advance Fee Scam	6	40	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Nigerian Round-Tripping Investigation	7	32	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Non-Profit Organization Operating as Money Remitter	7	31	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Operation Cheque mate	9	31	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Operation Mule Train	1	18	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Organized Crime Network	1	18	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Owner of Service Company Sentences in Tax Evasion Scheme	9	36	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Phantom Bank Scheme	2	30	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Ponzi Scheme	2	26	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Ponzi Scheme	7	31	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Securities Dealer	2	28	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Sports Betting Ring	3	31	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Sports Card Theft	3	32	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Stock Fraud	1	21	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Stolen Check Ring	3	32	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Stolen Check Scheme	2	31	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Structured Deposits Exceeding \$700,000	7	34	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Structuring and Food Stamp Fraud	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Structuring by Three Family Members	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Suspect Sentenced to Five Years in Prison & Ordered to Pay \$1 Million in Restitution	9	35	http://www.fincen.gov/sarreviewissue9.pdf
Law Enforcement Case: Tax Evasion Case	4	38	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Tax Evasion by a Business Owner	8	27	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Telemarketing Fraud	7	33	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Terrorism Investigation	8	25	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Travel Agent	2	29	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Unlicensed Money Remitter (\$1.2 million)	6	40	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Unlicensed Money Remitter (\$3 million)	5	52	http://www.fincen.gov/sarreviewissue5.pdf

Law Enforcement Case: Unlicensed Money Remitter (\$427,000)	5	51	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Unlicensed Money Transmission Scheme	4	35	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Unlicensed South American Money Exchanger	7	32	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Worker's Compensation Fraud	1	20	http://www.fincen.gov/sarreviewforweb.pdf
Life Insurance: SAR Analysis – Indications of Suspicious Activity	5	35	http://www.fincen.gov/sarreviewissue5.pdf
Mailbag and Feedback	6	79	http://www.fincen.gov/sarreviewissue6.pdf
Mailbag & Feedback – Review of BSA/Structuring/Money Laundering Violation on SAR Forms	7	53	http://www.fincen.gov/sarreviewissue7.pdf
Mailbag – Questions from the Industry	3	49	http://www.fincen.gov/sarreviewissue3.pdf
Money Services Businesses: SARs filed by MSBs	4	33	http://www.fincen.gov/sarreview082002.pdf
Money Transmitter Activity	2	18	http://www.fincen.gov/sarreview2issue4web.pdf
Money Transmitters may be Money Laundering Vehicle	3	17	http://www.fincen.gov/sarreviewissue3.pdf
Multilateral Illicit Currency Flows Study	2	23	http://www.fincen.gov/sarreview2issue4web.pdf
Non-Cooperative Countries and Territories	3	27	http://www.fincen.gov/sarreviewissue3.pdf
Non-Cooperative Countries and Territories	2	22	http://www.fincen.gov/sarreview2issue4web.pdf
Non-Cooperative Countries and Territories	1	15	http://www.fincen.gov/sarreviewforweb.pdf
On-line and/or Internet Banking	6	27	http://www.fincen.gov/sarreviewissue6.pdf
Pawn Brokers: SAR Analysis – Indications of Suspicious Activity	5	33	http://www.fincen.gov/sarreviewissue5.pdf
Percentage of SARs Reporting Structuring	3	25	http://www.fincen.gov/sarreviewissue3.pdf
Pre-paid Telephone Cards	2	19	http://www.fincen.gov/sarreview2issue4web.pdf
Real Estate Industry – Sales and Management SARs	6	31	http://www.fincen.gov/sarreviewissue6.pdf
Refund Anticipation Loan (RAL) Fraud	7	15	http://www.fincen.gov/sarreviewissue7.pdf
Regional Money Remitter Activity	1	13	http://www.fincen.gov/sarreviewforweb.pdf
Reports of Solicitation Letters (Advanced Fee Fraud or 4-1-9 Scams)	3	23	http://www.fincen.gov/sarreviewissue3.pdf
Role of SARs in High Risk Money Laundering and Related Financial Crime Areas	1	14	http://www.fincen.gov/sarreviewforweb.pdf
Russian Criminal Activity	1	12	http://www.fincen.gov/sarreviewforweb.pdf
SAR News Update: Expansion of PACS	6	67	http://www.fincen.gov/sarreviewissue6.pdf
SAR News Update: Expansion of SAR and AML Compliance Requirements to New Industries	4	46	http://www.fincen.gov/sarreview082002.pdf
SAR News Update: Expansion of SAR Requirements to New Industries	5	61	http://www.fincen.gov/sarreviewissue5.pdf
SAR News Update: Financial Industries Required to File SARs	6	69	http://www.fincen.gov/sarreviewissue6.pdf
SAR News Update: FinCEN's Financial Institutions Hotline	4	45	http://www.fincen.gov/sarreview082002.pdf
SAR News Update: Non-Cooperative Countries and Territories	6	68	http://www.fincen.gov/sarreviewissue6.pdf
SAR News Update: Proposed Revision to Suspicious Activity Report	5	62	http://www.fincen.gov/sarreviewissue5.pdf

SAR News Update: USA PATRIOT Act: Section 311 Authority	5	62	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Computer Intrusion and Frequently Asked Questions	3	38	http://www.fincen.gov/sarreviewissue3.pdf
SAR Tips: Definitions and Criminal Statutes for SAR Characterizations of Suspicious Activity	7	39	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Filing a Corrected or Amended SAR	4	42	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: Filing a SAR for Ongoing or Supplemental Information	4	43	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: Frequently Asked Questions Received on FinCEN's Regulatory Helpline	8	29	http://www.fincen.gov/sarreviewissue8.pdf
SAR Tips: How do I...?	7	38	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Identity Theft and Pretext Calling	3	41	http://www.fincen.gov/sarreviewissue3.pdf
SAR Tips: Importance of Accurate and Complete Narratives	5	55	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Importance of the Narrative	2	32	http://www.fincen.gov/sarreview2issue4web.pdf
SAR Tips: Improvements to Eliminate Reporting Deficiencies	6	49	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: Informal Value Transfer System--Special SAR Form Completion Guidance	5	57	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Insignificant Suspicious Activity Report Filing Errors	9	42	http://www.fincen.gov/sarreviewissue9.pdf
SAR Tips: Instructions for Completing the SAR Form	6	50	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: Problems with Taxpayer Identification Numbers	9	39	http://www.fincen.gov/sarreviewissue9.pdf
SAR Tips: SAR Filing Tips for MSBs	4	42	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: SAR Form Completion Rate-National Overview	1	25	http://www.fincen.gov/sarreviewforweb.pdf
SAR Tips: SAR Form Preparation and Filing	1	24	http://www.fincen.gov/sarreviewforweb.pdf
SAR Tips: SAR Forms: Where to Send Completed SAR Forms	5	58	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: SAR Forms: Where to Send Completed SAR Forms	6	57	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: SAR Guidance Package	7	37	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Special Guidance Related to Identity Theft and Pretext Calling	2	34	http://www.fincen.gov/sarreview2issue4web.pdf
SAR Tips: Suspicious Activity at a Location Other than the Institution	9	40	http://www.fincen.gov/sarreviewissue9.pdf
SAR Tips: Suspicious Activity Reporting Guidance for Casinos	7	37	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Suspicious Activity without a Loss to the Institution	9	41	http://www.fincen.gov/sarreviewissue9.pdf
SAR Tips: Terrorist-Related Activity: How to report potential terrorist-related activity	6	53	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: Terrorist-Related Activity: How to report potential terrorist-related activity	5	55	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Terrorist-Related Activity: How to report potential terrorist-related activity	4	41	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: Tips from the Regulators	6	54	http://www.fincen.gov/sarreviewissue6.pdf
SARs filed by Money Services Business	5	48	http://www.fincen.gov/sarreviewissue5.pdf
SARs Filed Referring to Terrorism (Prior to 09/112001 & 09/112001 through 03/31/2002)	4	25	http://www.fincen.gov/sarreview082002.pdf
SARs Filed that Refer to Terrorism (March -September 2002)	5	21	http://www.fincen.gov/sarreviewissue5.pdf

Suspicious Activity Reports for Securities and Futures Industries	9	5	http://www.fincen.gov/sarreviewissue9.pdf
Securities Industry: SAR Analysis - Indications of Suspicious Activity	5	38	http://www.fincen.gov/sarreviewissue5.pdf
Securities and Futures Industries SARs: The First Quarter	6	23	http://www.fincen.gov/sarreviewissue6.pdf
Shell Company Activity	1	11	http://www.fincen.gov/sarreviewforweb.pdf
State and Local Law Enforcement Use of SAR Data	7	35	http://www.fincen.gov/sarreviewissue7.pdf
State and Local Law Enforcement Use of SAR Data	6	45	http://www.fincen.gov/sarreviewissue6.pdf
State and Local Law Enforcement Use of SAR Data	4	39	http://www.fincen.gov/sarreview082002.pdf
State and Local Law Enforcement Use of SAR Data	3	33	http://www.fincen.gov/sarreviewissue3.pdf
Suspicious Activity Reported by Casinos	1	13	http://www.fincen.gov/sarreviewforweb.pdf
Suspicious Automated Teller Machine (ATM) Activity	1	13	http://www.fincen.gov/sarreviewforweb.pdf
Suspicious Endorsed/Third-Party Checks Negotiated Abroad	7	11	http://www.fincen.gov/sarreviewissue7.pdf
Terrorist Financing Methods: Coupon Redemption Fraud	6	14	http://www.fincen.gov/sarreviewissue6.pdf
Terrorist Financing Methods: Hawalas	5	19	http://www.fincen.gov/sarreviewissue5.pdf
Terrorist Financing Methods: Informal Value Transfer Systems	5	17	http://www.fincen.gov/sarreviewissue5.pdf
Terrorist Financing Methods: Informal Value Transfer Systems - Update	6	6	http://www.fincen.gov/sarreviewissue6.pdf
Terrorist Financing Methods: Non-Profit Organizations	5	21	http://www.fincen.gov/sarreviewissue5.pdf
Terrorist Financing Methods: SAR Filers Identify Suspicious Monetary Instruments Clearing Through International Cash Letters	6	12	http://www.fincen.gov/sarreviewissue6.pdf
Terrorist Financing: Aspects of Financial Transactions that May Indicate Terrorist Financing	4	17	http://www.fincen.gov/sarreview082002.pdf
Terrorist Financing: Financial Action Task Force (FATF) Efforts	4	27	http://www.fincen.gov/sarreview082002.pdf
Terrorist Financing: FinCEN Analysis of SAR Filings and other BSA information	4	19	http://www.fincen.gov/sarreview082002.pdf
Terrorist Financing: Reconstruction of Hijacker's Financial Activities	4	18	http://www.fincen.gov/sarreview082002.pdf
Terrorist Financing: Terrorism and Terrorist Financing	6	3	http://www.fincen.gov/sarreviewissue6.pdf
Terrorist Financing Suspicious Activity Reports	8	5	http://www.fincen.gov/sarreviewissue8.pdf
Travel Industry: SAR Analysis - Indications of Suspicious Activity	5	25	http://www.fincen.gov/sarreviewissue5.pdf
USA PATRIOT Act 314(a) Progress Report (February 2003 - October 2003)	6	37	http://www.fincen.gov/sarreviewissue6.pdf
USA PATRIOT Act 314(a) Progress Update (February 2003 - May 2004)	7	29	http://www.fincen.gov/sarreviewissue7.pdf
Use of Traveler's Checks to Disguise Identities	3	22	http://www.fincen.gov/sarreviewissue3.pdf
Use of U.S.-Based Shell Corporations and Foreign Shell Banks by Eastern Europeans to Move Money	7	3	http://www.fincen.gov/sarreviewissue7.pdf
Voluntary SAR Filings	3	26	http://www.fincen.gov/sarreviewissue3.pdf
Voluntary SAR Filings	2	19	http://www.fincen.gov/sarreview2issue4web.pdf

