The SAR Activity Review

Trends Tips & Issues

Issue 14

Published under the auspices of the BSA Advisory Group.
October 2008

The SAR Activity Review

Trends Tips & Issues

Issue 14

Published under the auspices of the BSA Advisory Group.
October 2008

Table of Contents

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

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

Introduction

The SAR Activity Review – Trends, Tips & Issues is a product of continuing dialogue and close collaboration among the nation's financial institutions, law enforcement officials, and regulatory agencies[1] to provide meaningful information about the preparation, use, and value of Suspicious Activity Reports (SARs) and other BSA reports filed by financial institutions.

This edition addresses several noteworthy topics. Several articles focus on the regulatory use of BSA data by federal and state regulatory agencies. An industry viewpoint addresses Identity Theft in the Industry Forum section.

Law enforcement cases in Section 3 demonstrate how important and valuable Bank Secrecy Act (BSA) data is to the law enforcement community. Many of these cases, which range in topic from a mortgage-related Ponzi scheme to medical fraud, were proactively initiated as a result of BSA report filings.

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

As always, your comments and feedback are important to us. We have included a feedback form in Section 6; please take a moment to let us know if the topics chosen for this issue are helpful.

---

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

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

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

Barbara Bishop
Regulatory Outreach Specialist
Financial Crimes Enforcement Network (FinCEN)
Phone: 202-354-6400
barbara.bishop@fincen.gov or
sar.review@fincen.gov

Section 1 — Director's Forum

This fourteenth edition of *The SAR Activity Review - Trends, Tips & Issues* is going to print as considerable changes are affecting the American financial sector. In these times of volatility in the financial market, it is important that we not lose sight of our anti-money laundering/ counterterrorist financing (AML/CFT) responsibilities. Recent events have only underscored the relevance of our AML/CFT framework. First, traditional distinctions between different financial industry sectors such as banking and securities markets have become increasingly blurred. Second, the global interconnections of the financial markets are beyond dispute. Third, there is a renewed focus on knowing one's customer for assessing creditworthiness and risks of fraud. These commercial incentives can and should be leveraged to carry out AML/CFT responsibilities.

Criminals and terrorists do not respect the law; they certainly do not respect national borders. They will seek to exploit the weakest link to move and launder money through any means of financial intermediation. As the readers of this *Review* certainly understand, our efforts to root out illicit financial activity increase confidence in and promote the integrity and stability of the financial system. These are critical contributions to helping the banking system return to what it does best, i.e. promoting legitimate economic activity and growth.

There are steps financial institutions can take to focus their resources and combat financial crimes. Last month, I gave a speech to the Florida Bankers Association where I discussed ideas that are gaining interest in the industry on the overlap of a bank's anti-fraud and anti-money laundering (AML) efforts. In the case of fraud, financial institutions have a clear interest in expending significant resources to combat this crime because there is a tangible impact on an institution's bottom line. In actuality, acts of fraud and acts of money laundering are interconnected: the financial gain of the fraudulent activity ultimately needs to be integrated into the financial system. When you fight fraud, you fight money laundering. By identifying money laundering, law enforcement can be alerted to criminal attempts to mingle the proceeds of fraudulent activity committed against innocent victims – some of

whom are certainly consumers of financial services products. I am hopeful that more and more financial institutions will recognize that the resources dedicated to AML programs are as important as those committed to fighting fraud. I encourage you to read my full remarks found at www.fincen.gov and I look forward to your comments and feedback. I expect that this topic will be of increasing interest in the months to come.

The Bank Secrecy Act requires, "*certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counter intelligence activities, including analysis, to protect against international terrorism.*" A major focus of this edition of the *Review* is how state and federal regulators are using Bank Secrecy Act (BSA) information to identify not only criminal activities but also to gain insights on the safety and soundness practices of an institution. FinCEN, by listening to feedback, is providing more tailored and state-specific information to our regulatory partners. In May 2007, FinCEN developed and disseminated its first BSA profile packages to the state officials with which it has information sharing agreements. At the same time, we made versions of these available to the public on our website as part of the companion to this publication, *The SAR Activity Review – By the Numbers*. Officials from the state banking departments of Nebraska and Oklahoma have provided articles that detail how they use the BSA data in their regulatory and enforcement roles.

Also included are articles from the Internal Revenue Service's Small Business/ Self-Employed (IRS SB/SE) stakeholder liaison and the Federal Deposit Insurance Corporation (FDIC). The IRS article discusses the ways that BSA information is used to identify and promote the registration of Money Services Businesses (MSBs). The FDIC article provides interesting details about how BSA information is used in non-supervisory ways. One example is its use to recover assets lost to insider fraud.

In the *Industry Forum*, John Byrne from Bank of America provides incisive comments on the fast-approaching requirements of the Fair and Accurate Credit Transactions Act (FACT Act). FinCEN has been collecting SARs related to identity theft for some time and will work closely with law enforcement to put this additional information which Congress requested to good use.

As always, this *Review* provides outlines of many more law enforcement cases that describe the successful use of SARs, Currency Transaction Reports (CTRs), Forms 8300 and other reports filed by banks, credit unions, casinos and the other industries that have BSA responsibilities to combat crime. Of special note, I think you will enjoy the case where a criminal actually laundered money, to include washing and ironing, to mask its suspicious odor.

These examples show the importance of FinCEN's unique role in spotting criminal movement of money through many different types of financial intermediation. The broad range of financial activities they cover make clear why Congress chose to centralize AML/CFT regulation and oversight into one expert agency. In these volatile times, this focused expertise will continue to serve the country well.

Again, I sincerely look forward to your feedback and comments.

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

Section 2 - Trends & Analysis

This section of *The SAR Activity Review* focuses on the use of BSA data by regulatory agencies. An article by FinCEN's Office of Regulatory Analysis illustrates how feedback from state regulatory agencies has resulted in enhancements to the annual BSA Data Profiles FinCEN prepares for many states. Officials from two States, Nebraska and Oklahoma, provide additional insight into just two of the ways BSA data is being utilized by state regulatory agencies. Also in this section, representatives from the Federal Deposit Insurance Corporation (FDIC) and an office of the Internal Revenue Service (IRS) Small Business/Self Employed Division discuss how BSA data supports each agency's regulatory mission.

2008 State BSA Data Profiles: Valuable Feedback from States Results in Significant Enhancements

By FinCEN Office of Regulatory Analysis

FinCEN is committed to supporting regulatory agencies that examine financial institutions for Bank Secrecy Act (BSA) compliance. Many readers may be aware of FinCEN's information sharing agreements with state and federal regulatory partners; since June 1, 2005, FinCEN has entered into Memoranda of Understanding (MOU) information-sharing agreements with 46 state supervisory agencies located in 42 states and one territory.

In negotiating information-sharing agreements with state supervisory agencies, FinCEN recognizes the growing importance of each state's capacity to ensure compliance with federal and state laws and regulations to protect the U.S. financial system from the abuses of financial crime. FinCEN pledges to provide state regulatory agencies with advanced analytic products intended to improve the overall effectiveness of BSA administration and expand the use and value of BSA data in systematic analysis and targeting. Based on the analyses, state regulators may adjust resources and investigate certain financial activity occurring in various locations within the state.

In May 2007, FinCEN developed and disseminated the first state-specific *Bank Secrecy Act Data Profile* packages for state supervisory agencies with which it has information-sharing agreements. A four-section, 26-page product highlighted BSA filing trends and patterns within those states through December 31, 2006. FinCEN received positive feedback from various state agencies for the 2007 effort and, as a result, plans to continue to provide this product annually.

New content was added to the 2008 State BSA Data Profiles, partially based on feedback from last year's products. The 2008 packages include enhanced and expanded exhibits incorporating intricate graphing, thematic mapping, and infusing of statistical data to depict each state's suspicious activity and currency transaction reporting trends. This year's product integrates current U.S. Census Bureau population data, which augment BSA data for each state. This edition adds maps illustrating national Suspicious Activity Report (SAR) filing trends and new trends analysis exhibits dedicated to mortgage loan fraud, filing patterns of Currency Transaction Report (CTR) and Currency Transaction Report by Casinos (CTR-C) filings, and graphical representations of registered and possible unregistered money services businesses (MSBs). The 46 profiles, and analysis developed for those states and territories without MOUs with FinCEN, were aggregated into consolidated packages and also provided to the Federal banking agencies and the IRS.

Profile Specifics

Each profile package is divided into sections, each with a specific focus and containing multiple exhibits displaying visual representations of the data. For example, certain sections provide exhibits illustrating reporting trends and comparison data for depository institution SARs filed from April 1, 2006 through December 31, 2007.[2] Enhancements this year include individual state and national ranking maps based on SARs filed in 2007 and state SAR filing trend comparison graphs displaying the percentage change in filings from April 1996 through the end of 2007. Some profiles drill down further into the data by incorporating geographic pattern maps that zoom-in to that state's largest urban areas.

2. Data retrieved through a financial database search of depository institution SARs. The maps are populated using zip codes appearing in SAR records.

The profiles include the top characterizations of suspicious activity reported by depository institutions in the state, including national geographic pattern and state thermal maps that provide volume data and hot spots for the top three types of suspicious activity. Also included are national and state maps depicting the subject address locations found in the 2007 SARs reporting mortgage loan fraud and state ranking maps relative to the SARs and each state's population.[3] A mortgage loan fraud SAR filing trend graph from April 1996 through 2007 is included.

Graphs depicting CTR filing trends and aggregate cash-in and cash-out transaction totals in the state for a 6-year period are included in the packages. If the state has casino operations, an additional exhibit shows CTR-C volumes and the percentage change from 2002 through 2007. For states that have casino and card club operations, another section is devoted to SARs filed by these operations, including a trend graph showing reporting volumes and percentage change for forms filed from August 1, 1996 through December 31, 2007.

Finally, the profiles include a series of maps identifying locations of MSBs registering with FinCEN during 2005-2006 and 2007. Maps showing the locations of unregistered MSBs identified by FinCEN analysts based on depository institution SARs for the same time periods are also included. A final graph depicts possible unregistered MSBs operating within the state by volume, total SARs filed, and total depository institutions filing these SARs in 2007.

Feedback

Improvements in this year's profiles directly resulted from constructive feedback FinCEN received from state regulatory agency representatives regarding the usefulness of last year's packages. One state representative found value in the state-by-state comparisons, particularly when adjusted for the population. A representative from one of the Federal banking agencies commented that "having separate data profiles for each state makes it convenient to distribute the data to their respective regions." FinCEN remains dedicated to providing useful analytic products to regulatory partners that rely on BSA information to manage and mitigate vulnerabilities associated with financial crime and will continue to improve these products based on customer satisfaction surveys and other feedback.

3. FinCEN created the national ranking maps by infusing SAR data with state population data obtained from the U.S. Census Bureau Annual Estimate of 2007.

Use and Protection of BSA Data Are Important to Nebraska Regulator

By John Munn, Director, Nebraska Department of Banking and Finance

The Nebraska Department of Banking and Finance enjoys direct access to Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and CTR exemption data through FinCEN. The information is invaluable in all of the Department's examination processes and licensing functions.

The Department monitors SAR activity among our state-chartered banks on an ongoing basis and each month, SARs are downloaded, printed, and reviewed by legal staff for suggestions of criminal wrong-doing. After gaining approval from FinCEN and the Nebraska State Patrol, a SAR may be referred to the Nebraska Attorney General for follow-up with the county attorney.

In supervising mortgage and payday lending, direct access to the FinCEN data base allows the Department to know more about parties seeking licenses than would be possible without the data. Knowing a SAR exists, the Department may elect to return an application with a broad request for more information regarding past activities.

Nebraska also uses the BSA data during the evaluation process for executive officers. Nebraska is unique among states in licensing executive officers of state-chartered banks. An executive officer's license (EOL) is required for any bank employee who makes loans, invests on behalf of the bank, may hire and fire bank employees, or exercises major policy authority. In evaluating an EOL application, we determine whether any SARs have been filed relative to the candidate. We fully understand that the existence of a SAR is not evidence. If a SAR exists, we treat it as a possible indicator of the need for further fact-finding, not as an indication of any wrongdoing. To uphold SAR confidentiality rules, we do not disclose the SAR or any information concerning the existence of the SAR.

With great tools comes great responsibility. Department policies make certain that the BSA data to which we have access is carefully safeguarded. Only four of our Department staff have access to the BSA site. The four received FinCEN training, underwent a security check and were finger-printed. Downloaded BSA data files are delivered to the BSA examiner by encrypted email; the email is deleted and the

email trash is emptied. At the conclusion of the examination, the file is deleted and trash emptied on the receiving computer. The information is never placed on a shared drive.

All records are stored on hard drives that employ full hard drive encryption. If retention of SAR data is needed after concluding a bank examination, select reports are printed and the electronic record destroyed. The printed records are assigned to an administrative assistant or examiner who keeps the documents under lock and key and makes them available as necessary to staff attorneys and review examiners.

Our Department is committed to handling the BSA data in line with the security and confidentiality safeguards required by FinCEN. We view FinCEN audits as an opportunity to enhance our understanding of FinCEN's expectations for safeguarding this valuable data.

BSA Data Assists Oklahoma in MSB Licensing

By Dudley Gilbert, Oklahoma State Banking Department

The Oklahoma State Banking Department began licensing money transmitters in 2007 in cooperation with the Oklahoma State Bureau of Narcotics and Dangerous Drugs Control ("OBN"). Oklahoma law requires the OBN to conduct a "criminal financial check" on all applicants for a money transmitter license, and requires the applicant to pay a separate fee to OBN for such background reviews. As part of the licensing process, information is collected on all directors and managing officers of an applicant and is used by the OBN to review not only an individual's criminal record but also information that may have been recorded in SARs filed with FinCEN.

Upon completion of the background review, OBN sends a report to the Banking Department listing criminal convictions as well as the number of SARs that may have been filed with respect to the applicant's managers and directors. The Banking Department may conduct further investigations on the individual, including contacting FinCEN to obtain copies of the actual SARs that have been filed. The Banking Department does not take any adverse action based solely upon the suspicions expressed in a SAR, but uses this information to investigate and reach an independent judgment about license applicants.

In addition to the background review at the time of application, any new managing officer and director must complete a form authorizing a financial background review as part of the annual license renewal process. These reviews give the Banking Department information that it may use when determining whether a licensee's managers and directors have the competence, experience, character, and general fitness to permit the applicant to engage in money transmission in Oklahoma.

SAR Data Assists IRS in MSB Registration Outreach and Education

By IRS SB/SE Stakeholder Liaison-BSA/Special Programs

In the May 2007 issue of *The SAR Activity Review* (Issue 11), FinCEN published findings from a comparative analysis of depository institution SAR filings on potentially unregistered MSBs. FinCEN continues to analyze these SAR filings monthly to identify potential unregistered MSBs and refers lists of entities to the IRS SB/SE Stakeholder Liaison (SL) Bank Secrecy Act (BSA)/Special Programs Team for outreach and education. This analysis is not initiated specifically for examination purposes. Rather, the lists of potentially unregistered MSBs are used to reach out to individual businesses and targeted geographic locations for educational purposes. This article is a follow up to the May 2007 article and reflects what has been learned through outreach efforts.

IRS outreach results based on the analysis of potentially unregistered MSB for August 2007 to December 2007 are illustrated in the table below.

FinCEN List	*Letter Returned Undelivered*	*Unable to Contact*	*Registered MSB or Contact Resulted in Registration*	*Exam Referral Warranted*	*Not Required to Register*	*Totals*
Aug-07	14	70	54	17	79	234
Sep-07	13	55	41	12	56	177
Oct-07	10	56	42	22	85	215
Nov-07	6	69	36	8	111	230
Dec-07	4	74	65	4	56	203
Totals	47	324	238	63	387	1059
% of Total	**4.4%**	**30.6%**	**22.5%**	**5.9%**	**36.5%**	**100.0%**

Unable to Contact

"Unable to Contact" includes entities with mail returned undeliverable or entities that IRS BSA specialists could not contact by telephone. Of the 1,059 potentially unregistered entities, 371 or 35% of the entities, could not be contacted. Of these, 47 letters were returned as undeliverable. The number of entities that could not be contacted suggests that many entities within the MSB industry are small and/or relatively new businesses susceptible to bankruptcy, business closures, and/or product and service shifts. This type of outreach is relatively new to FinCEN and the IRS. As we continue to streamline the analysis and outreach process to contact potentially unregistered MSBs in a timelier manner, we believe this percentage will decline.

Registered MSB or Contact Resulted in Registration

A total of 238 (22.5% of the entities) were already registered as MSBs or registered after the specialists guided them through the registration process during the contact.

Many MSBs are small, independently owned businesses offering money services as secondary business activities and many businesses may lack knowledge and understanding of the BSA filing and recordkeeping requirements. Although costly,

focused outreach to individual entities can have a lasting impact on this segment of the MSB industry. In particular, specialists found a need to educate check cashers in the following situations:

1. Some businesses have general policies limiting check cashing to under $1,000 for any one person on any one day, but the businesses will cash tax refund checks and economic stimulus checks during tax season. Often, these checks are more than $1,000, making the businesses cashing these checks subject to BSA requirements for MSBs.

2. Some businesses accept checks for payments of products and services and provide customers with differences in cash. These businesses are defined as MSBs if customers receive more than $1,000 back in cash or monetary or other instruments in one day.

On several occasions, MSBs received guidance from banks about registration requirements. Although banks often assist MSBs in complying with registration requirements, specialists identified the following examples where there was a misunderstanding of MSB registration requirements:

1. Some banks require MSBs to register when they are not required to do so, which results in processing and storing of inaccurate registration data. For example, some banks require businesses that only cash checks of less than $1,000, or that offer money services only as agents, to register.

   According to the MSB definition, businesses only cashing checks of less than $1,000 are not MSBs and are, therefore, not required to register. Similarly, businesses that are solely agents of other MSBs are not required to register. [Reference 31 CFR 103.11(uu) and 103.41(a)(2)]

2. Some banks incorrectly require MSB customers to register each "doing business as" (DBA) name, location and/or branch where customers provide money services. As a result, one MSB files several registration forms when the regulations require only one form.

   MSBs are not required to register each DBA name (Item 4 on Form 107). MSBs are also not required to separately register each location or branch. Form 107 instructions specifically state, "An MSB should not separately register each of its branches." An MSB should list the number of its branches in Item 25 on Form 107.

3. Some banks require customers to verify registration compliance. Accordingly, MSBs provide original registrations to these banks and assume the banks are filing registrations for them. Yet, the bank assumes the registrations are copies. As a result of miscommunication, the registrations are not properly filed with the U.S. Department of the Treasury.

   According to FinCEN guidance released in April 2005, MSBs are expected to provide confirmation of their FinCEN registration, if required, as well as their state licensing status, if applicable.

4. In some instances, banks have suggested that their MSB customers not cash checks of more than $1,000, and MSBs misconstrue this instruction to mean they are prohibited from cashing checks of more than $1,000. Specialists found that when businesses learn that the $1,000 threshold applies only to the MSB definition and not to business practices, they are willing to comply with registration and other BSA requirements.

5. Although FinCEN has issued guidance for banks and MSBs about maintaining relationships, some banks will not continue relationships with businesses offering check cashing, money orders, or money transfers.

Not Required to Register

A total of 387 (36.5% of the entities listed) were verified as offering money services solely in an agent/principal relationship and are therefore not required to register. IRS specialists found that in addition to banks, some companies issuing money orders and money transfers are incorrectly directing their agents to register. According to the BSA, businesses acting solely as agents of another MSBs are not required to register.

Examination Referrals

On occasion, entities refused to talk with specialists or to register when feedback from the entity indicated a registration requirement. These situations are referred to the IRS BSA Policy office for BSA examination consideration. Sixty-three, or 6% of the total, were referred for examination consideration.

Encounters with Law Enforcement

Specialists contacted a few business owners who faced criminal actions for not complying with the laws. One specialist was subpoenaed to testify at the individual's money laundering trial. The specialist's testimony helped the Assistant United States Attorney prove the defendant had sufficient BSA knowledge, and as a result, the defendant was convicted of 23 criminal counts for his role in a money laundering scheme.

Note: In March 2005, FinCEN and the Federal banking agencies (FBAs) issued guidance addressing the provision of banking services to MSBs, reiterating the AML compliance obligations for MSBs and assisting banking organizations in appropriately assessing and minimizing the risks associated with their MSB customers. FinCEN continues to work to address the issues and challenges facing the MSB industry as part of its regulatory efficiency and effectiveness initiatives. More information on these initiatives can be found on the FinCEN website at: http://www.fincen.gov/statutes_regs/bsa/bsa_effectiveness.html

Suspicious Activity Reports Valuable in Oversight Role of Federal Banking Agencies

By the Federal Deposit Insurance Corporation

A Suspicious Activity Report (SAR) is the primary means a bank has to alert law enforcement when an employee: (1) detects a known or suspected criminal violation of federal law; or (2) identifies a suspicious transaction related to money laundering activity or a violation of the Bank Secrecy Act (BSA). SARs are designed to elicit the type of information deemed beneficial to law enforcement's efforts to identify and investigate criminal activity. However, Federal banking agencies (FBAs) also benefit from the prompt recognition of suspected financial crime against or causing loss to a financial institution.

The public's confidence in the banking system is undermined when insured financial institutions are the victim of fraudulent and dishonest conduct which, through fidelity insurance premiums, can raise overall costs in the banking system. A review of SARs filed by an insured bank can alert the Federal Deposit Insurance Corporation (FDIC) to possible fraud. Prompt identification and follow-up of suspected fraud, whether internal or external, is vital to the strength of the banking system and maintenance of the Deposit Insurance Fund.

The FDIC's use of SARs goes beyond the BSA/Anti-Money Laundering (AML) examination process established to include internal procedures designed to identify activities and transactions warranting further review by supervisory staff and the FDIC's Office of Inspector General (OIG), Office of Investigations (OI), such as:

Supervisory Uses

Each FDIC region is responsible for developing and implementing a SAR review program that covers all FDIC-supervised depository institutions within their supervisory area. Given the high utility of database information, each region has adopted well-established procedures for obtaining SAR data and utilizing SARs in support of supervisory efforts, including the initiation and development of civil actions against individuals and referrals to law enforcement. By implementing a SAR management and tracking system, internal reviews identify those SARs involving institution-affiliated parties (IAPs)[4] or having material impact to the bank. After insider misconduct is brought to the FDIC's attention through the filing of a SAR, examiners generally conduct an extensive review of the alleged activities to determine if grounds exist to pursue an enforcement action and obtain evidence to support that action. Fraud perpetrated by employees, officers, or directors can be especially damaging and requires an expeditious supervisory response.

Moreover, insider fraud cases often reveal certain financial institution weaknesses with the primary failure being lax internal controls. In most cases, manipulation of bank records is discovered within a relatively short time, usually by internal auditors or bookkeepers but often by bank employees, including subordinates, who became suspicious of the subject's transactions. Early detection and reporting of fraud is key to limiting risk to an insured institution and the Deposit Insurance Fund. Prevention and detection of insider fraud are possible only through the vigilance of financial institution management and employees, examiners, and external auditors. Because cases are fact-specific and present unique circumstances, administrative remedies are determined on a case-by-case basis. Supervisory response to SAR reviews may involve several courses of action including coordination with the appropriate law enforcement agencies or other bank regulators; on-site visitation specific to an investigation that may result in a removal/prohibition action[5] or other formal enforcement action against an IAP or

4. Institution-affiliated party is defined in section 3(u) of the Federal Deposit Insurance Act (12 U.S.C. 1813(u))

5. §8(e) of the Federal Deposit Insurance Act (12 U.S.C. §1818(e)).

institution; on-site examination in response to activity that may impact the safety and soundness of the institution; and/or referral of apparent criminal violations conducted by IAPs to the FDIC's OIG/OI.

Investigative Uses

The FDIC's OIG/OI conducts investigations of activities that may harm or threaten to harm the operations or integrity of the FDIC or its programs. These investigations involve fraud at financial institutions, identity theft crimes, misrepresentations of deposit insurance coverage, and concealment of assets by FDIC debtors, among other criminal misconduct. The perpetrators of such crimes can be those trusted with governance responsibilities such as directors and bank officers, or individuals providing professional services to banks, and even customers themselves may be principals in fraudulent schemes.

The FDIC's OIG/OI coordinates closely with the FDIC's Division of Supervision and Consumer Protection in investigating fraud at financial institutions. OIG/OI also collaborates with the Division of Resolutions and Receiverships and the Legal Division in investigations involving failed institutions and fraud by FDIC debtors. The FDIC's OIG/OI criminal investigations also benefit the banking industry by pursuing enforcement actions to prohibit offenders from continued participation in the banking system.

Investigations for financial institution fraud represent approximately 85 percent of the FDIC's OIG/OI's current caseload. Responding to allegations of fraud and other financial crimes affecting FDIC-insured institutions referred to the OIG or identified through internal review and analysis of SAR filings has resulted in over 216 investigation actions in fiscal year 2007 alone, including indictments, convictions, informations, arrests, pre-trial diversions, criminal non-monetary sentencings, monetary actions, employee actions, and other administrative actions. As a result of cooperative efforts with U.S. Attorneys throughout the country, numerous individuals were prosecuted for financial institution fraud and successful outcomes resulted in combating a number of emerging mortgage fraud schemes during the past year.

As a result of the establishment of FinCEN's Web CBRS (Currency and Banking Retrieval System), submitted information including SARs, currency transaction reports (CTRs), and CTR exemptions may be obtained directly online from a secure database. Each FBA has staff authorized to obtain this data. The FDIC OIG/OI has capacity to search and sort data from FinCEN to assist in investigations and

supervisory enforcement actions. In the FDIC OIG Semiannual Report to the Congress (October 1, 2007 – March 31, 2008), the OIG reported investigative results leading to 78 indictments/informations, 42 convictions, and over $86 million in total fines, restitution, asset forfeiture, and monetary recoveries for the six-month period prior to March 31, 2008. Of note during this time, a 6-year investigation relating to a 2002 bank failure was concluded resulting in substantial prison terms and orders to pay $41 million in restitution. This report also presented a number of other successful investigations involving a growing number of mortgage fraud schemes, bank fraud, money laundering, and securities fraud. As previously reported earlier in 2007, several significant mortgage fraud cases were undertaken in partnership with the Federal Bureau of Investigation (FBI) and U.S. Attorneys' Offices resulting in stiff penalties for the offenders.

Currently, the FDIC OIG has initiated 126 open bank investigations involving an estimated $1.5 billion in potential fraud. More than 75% (three quarters) of these cases are being pursued jointly with the FBI. Additionally, OI maintains close and continuous working relationships with the U.S. Department of Justice; other Offices of Inspector General; and federal, state, and local law enforcement agencies.

Receivership Uses

The FDIC's Division of Resolutions and Receiverships (DRR) is responsible for the payment of deposit insurance proceeds to bank depositors. The DRR Investigations Unit is charged with thoroughly reviewing the activity of failed institutions. In completing this task, staff assesses the culpability of banks' directors, officers, and other staff as well as identifies and reports on criminal activity. Investigations also use SAR data for information to support possible fiduciary blanket bond claims. This bond is used to insure the bank against many types of criminal activities within the institution including actions of officers, employees, and borrowers. A SAR serves as a valuable document in the investigative stage.

DRR benefits by having the ability to search, obtain and review SARs that have been submitted by institutions that are on the verge of failure. DRR has the ability to file a claim against the bond, based upon the assumption there is knowledge of some type of fraud. Most insurance companies require notification of fraudulent activity prior to failure. Some insurance companies require a *proof of loss* with full detail before the institution fails. The SAR can provide needed information to help meet insurance company claim requirements. All policies have specific time frames in which a claim for *proof of loss* must be filed. Even though some insurance companies

have longer periods of time in which to file the claim, a notice letter must be sent to the bond company notifying them of a potential claim before the institution's failure. SARs have been invaluable in providing support for these letters.

Summary

While financial institutions principally submit SARs to FinCEN in order to comply with regulations issued by the five federal financial institutions supervisory agencies and the U.S. Department of the Treasury, many government agencies may benefit from this reporting. SARs assist federal and state law enforcement authorities with the identification or evidentiary support of criminal activity. Furthermore, SARs provide banking supervisory agencies with a means of early detection of fraud and other financial crimes that could lead to deterioration in an institution's financial condition or in the most severe circumstances weakening of the banking system. Industry efforts put into SAR preparation and their filing significantly aid the FDIC's supervisory and resolutions staff as well as the FDIC's OIG/OI in carrying out mission-critical objectives and safeguarding public confidence in the nation's financial system for all.

Section 3 – Law Enforcement Cases

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

Law Enforcement Contributors: As part of our efforts to preserve the confidentiality relating to SARs, while also maintaining our ability to provide information on the value of SARs to law enforcement, we do not link any SAR filings to the lead law enforcement agencies. Rather, we provide a general list of agencies and entities that utilized SAR information and other BSA data for the cases highlighted in this issue: The United States Attorneys for the Eastern Districts of California and Virginia, Northern Virginia SAR Review Team, ICE, DEA, USSS, SEC, FBI, IRS, USPIS and HHS.

Contributing Editors: Shawn Braszo, Johnna Pimentel, James Emery, John Summers, Jack Cunniff.

BSA Records Show Money Received through Mortgage-Related Ponzi Scheme Supported Million-Dollar Gambling Habit

A federal investigator characterized BSA data as extremely important in determining how the defendant in a multi-million dollar fraud case spent the proceeds. FinCEN researchers recovered almost 400 Casino CTRs related to the defendant dating back more than 10 years. Although some of the casino transactions pre-date the period of the fraud, investigators used the records to identify accounts and subpoena casino records.

According to the prosecutor, the defendant personally met with dozens of victims of the fraud, telling each that he would use their money to underwrite legitimate mortgages. Rather, their funds were put to use in keeping a massive Ponzi scheme afloat. The defendant collected more than $29 million in fraudulent investment in just 2 years, a significant portion of which was diverted to his gambling activities.

Evidence presented to the court chronicled how, as president of his own mortgage company, the defendant engaged in a scheme wherein he and others acting on his behalf solicited individuals, including business associates, personal friends and members of his church, to invest with him. The defendant informed his investors that he would use their money to underwrite safe and secure "bridge loans" for wealthy individuals who were selling a house and needed funds to use as a down payment on newly acquired real property or to assist real estate developers with their short-term capital needs. The defendant entered into short-term promissory notes with his lenders, the terms of which he dictated, to document their investments.

The defendant falsely represented that his investors' money would be secured by his borrowers' equity and would be repaid, with substantial interest, in a short period of time. Instead, he used his investors' funds to repay his principal and interest obligations to earlier investors and laundered more than $7 million of their assets to fund his gambling activities at casinos in Nevada, Mississippi, and New Jersey.

BSA records revealed the vast amount of money associated with the fraud, with transaction amounts reported by the casinos ranging from approximately $12,000 up to $150,000. A federal jury found the defendant guilty on charges of wire fraud and money laundering related to an investment scheme.

Proactive SAR Review Leads to Guilty Plea on Conspiracy and Money Laundering Charges

A Suspicious Activity Report detailing more than $4.6 million worth of fraudulent activity associated with electronics sales over the Internet prompted a SAR review team to initiate a case on a subject known to have been previously identified with fraudulent activity. The filer reported that the subject sold electronics through the Internet; however, a quarter of the subject's clients never received their purchases despite the credit card payments. Subsequently, investigators found additional SARs that detailed illicit activity on the part of the defendant.

The defendant, the former president of a company that sold electronic devices such as iPODs, Xboxes, PlayStations and cell phones over the Internet and by telephone, pleaded guilty to fraud and money laundering. The defendant admitted that he defrauded a credit card processing firm of more than $2 million worth of customer orders that his electronics business failed to fulfill.

At the plea hearing, the assistant U.S. attorney said the government could prove that, after incorporating the business, the defendant and another representative of his business submitted an application to a firm to process credit card transactions. As part of the application, the defendants prepared and submitted various supporting documents, including purported federal income tax returns for several years. Those returns falsely represented that the Internet business had gross receipts of more than $2 million in 2 years. In fact, their Internet business was not in operation during those years, and the defendant's actual federal tax returns for those years did not reflect any business income from an Internet firm.

The credit card firm processed millions of dollars worth of credit card transactions on behalf of Internet business for orders the company received from the defendants' business. When the defendants' Internet business ceased operations, hundreds of customers subsequently complained to the credit card firm that their credit card accounts had been charged for unfulfilled merchandise orders. The credit card firm refunded customers more than $3 million in charges for unfulfilled orders. The firm was able to recoup nearly $1 million from a bank, but was left with a net loss of over $2 million. Individual losses ranged from less than $100 to thousands of dollars.

The defendant pleaded guilty to one count of conspiracy to commit wire fraud and one count of money laundering. At sentencing he agreed to pay over $2 million in restitution.

SAR Review Team Identifies Gift Shop Operating as an Unregistered Money Services Business

A Suspicious Activity Report review team identified SARs filed by three different financial institutions within several months on the same subject, describing similar transactions involving structuring and the wire transfer of funds to an Eastern European country (Country A).

According to prosecutors, the defendant operated a gift shop as a money transmitting business that transmitted funds off-shore on behalf of the store's customers. In connection with this activity, the defendant would make large cash deposits into bank accounts he maintained at various banks. He then would initiate wire transfers from those accounts to Country A.

The defendant had been repeatedly advised orally and in writing by banking representatives that federal law required certain money transmitting businesses to register with FinCEN. Two banks closed his accounts when he failed to demonstrate that he was so registered or explain why he was not required to be registered and to either provide proof of registration or to adequately justify his non-registration. In response to these account closings, the defendant shifted his transmitting activities to other banks and continued to conduct the money transmitting business without registering with FinCEN in violation of federal law.

The case began with a proactive review of SARs conducted under the auspices of the United States Attorney's Office. The team found that during 2005 three banks filed five SARs on the defendant. All three banks noted that the defendant structured cash deposits to his accounts and wired the funds to Country A. One bank subsequently closed the accounts; a second bank filed SARs on similar activity a few months after the first bank closed the defendant's accounts even though the defendant assured bank representatives that he would not be using his new account for any MSB activity or wire transfers. The banks also noted that the defendant's business was not registered as an MSB with FinCEN.

The defendant is also the subject of five CTRs and a Form 8300, Report of Cash Payments Over $10,000 Received in a Trade or Business. The cash payment report documented that he made a down payment of over $20,000 in cash, with mostly hundred dollar bills, for the purchase of an automobile.

In early 2008, a United States Attorney announced that the defendant pleaded guilty to conducting an unlicensed money transmitting business in violation of federal law requiring the registration of such businesses. The defendant received a 1-year sentence and 2 years of supervised release. When sentencing the defendant, the Court commented on the fact that the defendant had been repeatedly advised by banking institutions that it was illegal to conduct a money transmitting business without registering with FinCEN, yet he nonetheless continued the activity by shifting it to different banks.

Restaurant Owner Pleads Guilty to a Charge of Structuring Bank Deposits

In a case started by a Suspicious Activity Report review team, investigators charged a restaurant owner with structuring bank deposits. The subject had been known to law enforcement for some time, and local authorities suspected him of participating in illegal activity. The resulting investigation determined that the subject structured deposits into three accounts at two banks, and both banks filed SARs on the transactions.

The defendant in this particular case owned and operated a restaurant that was known to various local law enforcement agencies as a location involved in the receiving and selling of stolen property and drug sales. The restaurant eventually became the focus of a property crime task force set up to combat the rising number of property crimes in the area. In the course of the investigation, police made numerous arrests and recovered a significant amount of stolen property from various subjects visiting the restaurant. However, no charges against the defendant were filed at that time.

Subsequent to the above arrests, the defendant's name appeared again when a SAR review team was reviewing potential structuring violations and unlicensed money services businesses reported through SARs filed in the local area. Investigators found four structuring SARs on the defendant, filed by two different banks. The defendant structured deposits into the two banks at the same time, and both banks filed SARs for that activity.

The SARs reported that the defendant owned and operated another restaurant, however he could not validate his claim that the structured cash came from his restaurant food sales. During an interview with the defendant, investigators were able to prove that he structured cash transactions to avoid currency transaction reports, thus leading to the charge of structuring as well as to the forfeiture of the funds that had been seized during the investigation.

The defendant waived indictment and pled guilty to a criminal charge of a single count of structuring transactions to evade U.S. Treasury reporting requirements. In a statement of facts, prosecutors detailed 47 suspect transactions that occurred within a 2-month period, as well as 13 transactions during a 2-week period a year later. The defendant was also the subject of 10 CTRs filed prior and up to the date of the first SAR. As part of his plea agreement, the defendant admitted depositing nearly $400,000 in cash, in amounts of $10,000 or less, in an attempt to evade transaction reporting requirements.

The defendant consented to the forfeiture of over $20,000, which the government seized during its investigation. The defendant also filed amended tax returns as part of his plea. The probation officer reported that the amendments reflected a net change in his income of over $200,000, resulting in more than $80,000 in taxes owed.

BSA Documents Lead to Repatriation & Seizure of over $9 Million Generated by Illegal Internet Pharmacy

In 2005, a federal task force initiated a 2-year multi-agency investigation against an online pharmaceutical distribution network, resulting in indictments against 18 individuals. The investigation was based on information received from a cooperating witness, who alleged that a pharmaceutical network sold controlled and non-controlled prescription drugs through numerous affiliated websites to customers without an authorized prescription.

A SAR filed by a financial institution detailed over 225 wire transfers, totaling over $4.8 million, through correspondent accounts. The SAR helped identify bank accounts that were the focus of the asset removal portion of the investigation. Over $9 million has been repatriated from overseas accounts and seized by federal agencies as part of the forfeiture proceedings.

The pharmaceutical network website was in operation for almost 2 years. During this time, investigators made numerous undercover purchases of prescription drugs. Additionally, the pharmaceutical network allegedly received more than one million Internet orders for controlled and non-controlled prescription pharmaceuticals from the United States.

The pharmaceutical network paid licensed doctors from different states, as well as Puerto Rico, to review health questionnaires completed by online customers and to issue prescriptions based on those answers. In some instances, the network issued prescriptions for pharmaceuticals even when a customer's answers to the health questionnaire suggested that the drugs could pose a danger to the customer, or where the customer's medical condition did not require treatment.

In an attempt to evade federal law enforcement, the defendants situated the network headquarters in Central America and used computer servers in the Middle East. The company also relied on foreign-based agencies to process credit card payments. The company allegedly used various bank accounts and an accounting firm in the Middle East to distribute proceeds while attempting to conceal and protect the illicit proceeds from U.S. authorities. The accounting firm set up shell companies in overseas locations with associated shell bank accounts, putting only a limited amount of money in each account. The accounting firm reasoned that if U.S. law enforcement officials were to seize one bank account, the rest of the bank accounts would be safe. BSA information, however, assisted law enforcement in connecting these individuals to the various accounts connected to the activity.

Last year, a federal grand jury indicted the 18 individuals on 313 counts of racketeering, conspiracy to distribute controlled substances and conspiracy to commit money laundering for allegedly operating an Internet business that generated more than $126 million in gross revenue from the illegal sale of prescription pharmaceuticals to customers in 50 states. The defendants included physicians, pharmacists, a credit card processor, and affiliate website operators. Half the indicted individuals have pled guilty to date and the rest are awaiting trial.

SARs Lead to Recovery of Funds Derived from Medical Fraud

BSA records often play a crucial role in federal investigations of medical fraud. The records are often instrumental in seizing assets and shutting down businesses that may be perpetrating the fraud. Some of the businesses may exist on paper only, and prosecution of the perpetrators is often difficult and time-consuming. However, cooperation between the financial industry and government agencies, facilitated through Suspicious Activity Reports, results in early detection of medical fraud and swift action to seize funds generated through the illegal activity. Two recent cases highlight the value of BSA records in these types of investigations.

In one case, initiated through data analysis of fraudulent billing practices, agents discovered that a pharmacy was billing for items and in a manner that was highly consistent with known fraudulent practices. Investigators interviewed numerous individuals purported to be patients (beneficiaries) for whom the pharmacy submitted claims to the Medicare program for expensive respiratory medications used with durable medical equipment (DME). None of the beneficiaries interviewed had received any DME, nor did they know the physicians named as the referring physicians in the claims. Agents also interviewed several physicians whose names and Universal Provider Identification Numbers were used by the pharmacy in order to submit claims to Medicare. None of the physicians had ever prescribed the DME in question, and attested that the beneficiaries for whom they purportedly prescribed the DME were not their patients.

Two financial institutions filed SARs because of transactions involving the pharmacy's accounts that were inconsistent for such a business and notified authorities of the suspicious transactions. Information provided by the financial institutions helped agents obtain and execute a seizure warrant for over $1.3 million held in two corporate bank accounts titled to the pharmacy.

In a second case, initiated from a financial institution SAR, agents opened an investigation on a medical services "clinic" billing for a variety of anesthetic and back pain medical procedures. The physician listed as the treating doctor for the clinic was interviewed, as well as several beneficiaries. None of the beneficiaries interviewed had received any of the treatments that were billed to Medicare, been treated at the medical services business, or knew the physician listed as the treating doctor in the Medicare claims. The physician stated that he had never performed the procedures for the patients on whose behalf the medical services business submitted claims to Medicare, and attested that all of the claims made under his name were fraudulent.

The federal agency conducting the investigation obtained a warrant at a U.S. District Court for the seizure of funds frozen in the corporate account belonging to the medical services business. The seizure warrant led to the recovery of over $500,000.

BSA Records "Critical" in Conviction of Money Launderer in Organized Retail Theft Case

In a case that is part of a large-scale investigation into organized retail theft (ORT) rings, a federal jury convicted an individual of multiple counts related to laundering the proceeds from the criminal activity. Investigators found Suspicious Activity Reports filed on the defendant very useful in the case. Moreover, multiple banks examined activity related to the defendant, determined that it was suspicious and filed SARs. The bank also closed the defendants' accounts.

Evidence gathered in a joint investigation is credited with securing the conviction of a grocer on counts of failure to file currency transaction reports, conspiracy to commit money laundering, and money laundering. The grocer was convicted for his role in helping five ORT rings launder at least $69 million derived from the sale of stolen baby formula and health-and-beauty products. The conspiracy continued for 5 years and involved nearly 400 financial transactions.

In organized retail theft, street-level thieves, known as boosters, steal large quantities of over-the-counter drugs and health-and-beauty products from retailers. They sell the goods to repackagers who remove price tags and other markings indicating that the products are stolen. The stolen goods are then either sold directly to convenience stores or to wholesalers who mix the items with legitimately purchased products and sell them in large quantities to retailers and convenience stores.

Over the course of the conspiracy, the defendant accepted third-party checks for deposit and wire transfers to his business account from five different ORT rings. In turn, he provided cash to the organizations, minus his fee (of more than $600,000 in 5 years), generally paid through intermediaries. In an attempt to obscure transactions further, some of the ORT rings asked businesses purchasing their products to pay the defendant's business directly by check or wire transfer. The defendant registered his grocery as a money services business, potentially as a means to justify large-dollar wire transfer, check, and cash transactions through his store accounts.

A federal agent closely involved with the investigation called SARs associated with the case "critical" in identifying bank information about the defendant's business and in reporting some of the payments received by his business from some of the entities involved in the ORT. Several years earlier, a bank had filed a SAR noting that the defendant's account activity was not consistent with a typical food market operation. The bank subsequently closed the account.

The next year, another bank opened and closed an account affiliated with the defendant. Based on financial activity associated with the account, the bank determined that the associated business was operating as a money services business. The bank requested supporting documents, such as a copy of the MSB's license and anti-money laundering program. When the business could not provide the material, the bank closed the account.

The lack of CTRs documenting the cash the defendant's business paid to ORT rings triggered the counts of failure to file CTRs in the indictment. Additionally, the agent noted that the defendant had testified that he was unaware of his obligation to file CTRs when he provided large amounts of cash to ORT rings. This testimony was discredited by an examiner, who testified that he recalled instructing the defendant on BSA procedures related to the operation of an MSB as outlined in FinCEN-provided MSB materials seized from the defendant's business.

Prosecutors are seeking $4.8 million in forfeitures and money judgments. The defendant is also likely to receive a sentence of 5 to 9 years in prison.

Suspicious Activity Reports Describe Marijuana Traffickers' Attempt to Wash, Dry, and Iron "Dirty" Currency

Investigators looking into a large-scale international marijuana smuggling and money laundering operation received a break when two banks filed SARs on the targets. One bank filed SARs on structured deposits into a business account that held proceeds of the illegal operation. A second bank filed SARs that described the efforts the subjects made to apparently eliminate the smell of marijuana from currency deposits.

A United States Attorney announced that the defendant had been sentenced to 30 years imprisonment for his leadership role in a conspiracy that imported over a ton of marijuana and left at least two conspirators dead and another wounded. The defendant pleaded guilty in federal court to marijuana conspiracy, money laundering, and international money laundering. The defendant also admitted legal culpability for the death of another individual, the former leader of the drug conspiracy.

Multiple federal and state agencies successfully concluded a multi-year investigation of the marijuana importation and distribution ring. Other defendants in the case have received sentences ranging from 20 to 48 months. Additionally, the government seized several million dollars worth of assets, including currency, firearms, vehicles, and real property.

Local police became aware of the defendant's probable involvement in marijuana importation several years earlier as a result of information from a confidential informant in an unrelated drug investigation. At that time, the evidence against the defendant was judged to be insufficient to proceed with an indictment. His name resurfaced several years later following a cash deposit to his business account made by one of his employees. The teller receiving the deposit remarked that the cash smelled like marijuana. Branch employees reported the transaction to the bank's security department. The bank filed a SAR on the incident, and noted that currency received in subsequent deposits appeared to have been laundered and ironed. Another SAR noted an exchange between a bank employee and a prior employee of the defendant, who referred to a deposit of "dirty money." The SARs were instrumental in re-igniting law enforcement's interest in the defendant.

As the investigation progressed, investigators identified a murder victim as the prior head of the importation conspiracy, which involved four principals as well as others. Eventually, the murder victim and his partner handed over day-to-day operations of the organization to the defendant so that they could concentrate on providing financing and distribution contacts to the growing operation.

The investigation revealed that over the course of the conspiracy the organization imported and distributed more than 1,000 kilograms of marijuana into the local market. The drugs were concealed in hidden compartments in commercial trucks for importation. A measure of the profitability of the operation was evidenced by the murder victim's intended purchase of commercial real estate in an Eastern European country for $1 million cash. The defendant convinced his business partner to murder the head of the drug ring, leading to the defendant's control of the marijuana importation and distribution network.

SARs filed over several years revealed how the defendant and his business partner structured cash deposits on behalf of the organization. In addition, the records described transactions indicative of money laundering, such as the suspicious purchase of cashier's checks. The defendant also laundered some of the drug proceeds by paying the murder victim a salary, though he did no actual work.

One depository institution filed SARs describing activity related to the accounts of two parties involved in the investigation. Through an analysis of the accounts, the depository institution was able to determine that one party received numerous checks from the other party and also noted that the financial dealings of one involving an Eastern European country were extremely questionable because of the country's reputation for lax anti-money laundering practices.

SARs filed by a second bank contemporaneously and prior to those filed by the depository institution documented structuring of cash deposits into the defendant's business account there. The SARs, filed regularly over several years, detail transactions totaling as much as $500,000 in a 5-day period.

SARs Are Catalyst in Investigation of $13.1 Million Tax Fraud Conspiracy

Federal law enforcement agencies conducting a tax refund fraud investigation uncovered at least $13.1 million in fraudulently obtained federal and state tax refunds. The lead investigator in the case said the investigation began when a bank reported anomalous automated clearing house (ACH) credits received from federal and state revenue offices. The lead defendant pled guilty to conspiracy, wire fraud, and aggravated identity theft in the investigation. Other defendants had previously pled guilty to wire fraud. An Assistant United States Attorney indicated he was relatively certain that the remaining 14 defendants would also eventually plead guilty.

A year earlier, a United States Attorney announced an 18-count indictment naming 17 defendants for their alleged involvement in the tax fraud scheme. According to the indictment, conspirators stole identity information (including Social Security numbers), predominantly from elderly nursing home patients, and used it to prepare both federal and state tax returns using tax preparation software. Conspirators allegedly prepared false W-2 information, listing employers that the identity theft victims never worked for, false residence addresses, and other false information. The tax information on the returns was entirely fictitious, according to the indictment.

In order to conceal their true identities, the indictment alleges, conspirators filed these fraudulent tax returns electronically through public Internet "hot spots," such as coffee shops or restaurants, and through unsecured private wireless networks maintained by unwitting individuals with no connection to the conspiracy. Conspirators often paid the filing fees with credit cards or loadable debit-type cards, the indictment says, which were opened using identity theft victims' names.

According to the indictment, the false tax information was used to generate at least 365 federal refund claims ranging from $4,000 to $47,000 each. The indictment alleges that conspirators also submitted false returns to 27 state taxing agencies, typically in conjunction with federal returns, to generate claims in the range of $1,500 to $20,000 per return. According to the indictment, conspirators often filed multiple state tax returns in conjunction with a single federal tax return. Mail related to the returns and credit cards was sent to commercial mailboxes across the metropolitan area, the indictment says, and conspirators often used "runners" to pick up this mail in order to conceal their own identities.

Conspirators caused numerous bank accounts to be opened both locally and elsewhere, the indictment says, specifically for the purpose of receiving electronic fund transfers of tax refund payments. Shortly after a refund payment was wired into an account, conspirators allegedly used runners to help them withdraw the money. According to the indictment, conspirators wrote checks to the runners in amounts less than $10,000 and drove the runners from bank to bank to cash the checks until the accounts were depleted or the bank or the IRS detected the fraud and froze the account. The runners allegedly gave the withdrawn funds back to the conspirators and received a small payment for their services.

Some of the money obtained by the conspiracy was wired to banks in a foreign country, the indictment alleges, and on some occasions refund money was withdrawn directly from accounts through automated teller machine (ATM) withdrawals in that country. The indictment also alleges that the conspirators routed some electronic transfers of tax refunds directly to prepaid debit-like cards obtained anonymously through an Internet application process.

The conspiracy began to unravel when bank employees questioned the legitimacy of multiple large federal tax refunds deposited into the account of a co-conspirator, supposedly to benefit apparently unrelated individuals. The lead federal investigator in the case noted that most tax investigations are historical in that the illicit activities they concern are rarely ongoing. In this investigation, notification from the SAR filing bank, previous SAR filings, and filings made subsequent to a federally issued alert to area banks allowed law enforcement to track ongoing activities of many of the defendants. The investigator also credited the SAR filings with speeding up the investigatory process and limiting the need for numerous subpoenas in the case.

One of the Assistant US Attorneys assigned to the case credited associated SAR filings with quick identification of accounts receiving multiple ACH refunds or ACH refunds ostensibly filed for the benefit of legitimate taxpayers received in the accounts of defendants. The prosecutor also indicated that federal recovery of several hundred thousand dollars worth of fraudulently obtained refunds was made easier by SAR filings. Close cooperation between law enforcement agencies and the financial institutions associated with this investigation contributed to the successful prosecution of the case.

Proactive SAR Review Uncovers $15 Million Securities Conversion Scheme

Four federal law enforcement agencies coordinated an investigation of a long-running fraud conspiracy that netted its participants more than $15 million in illicit proceeds. The ringleader, a retired financial executive, and a friend concocted a scheme to use nominee buyers to purchase greater quantities of initial public offering (IPOs) shares than are permitted under federal and state banking regulations. Specifically, the issuers of these IPOs were mutual financial institutions converting from depositor to public ownership. The lead federal investigator in the case credited a SAR identified by a SAR Review Team and filed by one of these institutions with precipitating the investigation.

The lead defendant admitted that he implemented a scheme to open accounts at mutual financial institutions across the country with the knowledge that some of these institutions would eventually make IPOs. Several dozen institutions did so during the more than 11 years that the conspiracy continued. Federal and state banking regulations require that when a mutual bank makes an IPO it must apportion shares offered first to depositors, restrict the maximum number of shares offered to each depositor, and prevent depositors from transferring their shares to other depositors. In many instances, mutual financial institutions also require that depositors be residents of the state in which the institution is located.

The lead defendant circumvented IPO-related regulations by employing relatives, close friends, and apparently even bank employees, to open accounts at mutual banks. The co-conspirators got around the residency requirements by paying others to add them to a residential utility account, thus allowing them to establish state residency and fraudulently acquire valid state identification. In the event of an IPO, the aforementioned relatives and close friends acted as nominee buyers of the maximum allowed number of shares. The lead defendant provided the money to make the purchases. The buyer would then transfer this stock to one of the defendants' investment accounts. The defendants would generally sell this stock in the secondary market shortly after the IPO effective date, thus generally reaping large profits on an oversubscribed offering provided to depositors at a below-market price in the IPO. The most lucrative IPO netted the lead defendant more than $1 million profit. Since each of the IPOs in which the lead defendant and his nominee buyers bought stock was oversubscribed, this activity limited the ability of legitimate depositors to secure the maximum number of shares potentially available to them in the IPO, thus depriving them of greater potential profits.

A SAR review team identified the depository institution filing that sparked the investigation. Bank employees became suspicious when they noted wire transfers into one of the defendant's accounts and offsetting wire transfers and checks written out of his accounts aggregating to millions of dollars which the defendant could not adequately explain. The defendant also wrote millions of dollars worth of checks to open accounts at or to purchase IPO stock in mutual financial institutions. The bank filed the SAR because it believed that the defendants might be involved in a conspiracy to exceed the limits on the number of shares a depositor of a mutual financial institution can purchase in an IPO.

One defendant received a prison sentence of several years after pleading guilty to a single count of conspiracy to commit securities fraud. As part of his plea agreement, the defendant was also required to return more that $10 million of the funds illicitly derived from the scheme. Other defendants in the case received shorter sentences and were required to repay significant amounts of illicitly derived proceeds.

SAR Leads to Structuring Conviction for Mortgage Broker

A federal law enforcement investigation led to the conviction of a mortgage broker who structured more than $500,000 into multiple accounts at various financial institutions. As part of the defendant's guilty plea to structuring, he admitted that he structured specifically to avoid the Bank Secrecy Act's CTR filing requirements.

In 2005, the defendant made more than two dozen deposits at multiple branches of several different banks aggregating to nearly $300,000. More than a year later, he made numerous deposits through more than a dozen branches of a single bank totaling nearly $200,000.

One of the earliest-filed SARs was pivotal in helping investigators determine that the defendant was structuring multiple cash deposits and withdrawals to/from several accounts to stay under the CTR reporting limit. This SAR caught the attention of a federal law enforcement agent who was part of a SAR review team. An in-depth search for relevant BSA documents located numerous SARs filed by multiple financial institutions describing both cash structuring and the apparent structured purchase of money orders by or for the defendant.

Specifically, the key SARs revealed that during a brief period the defendant was structuring through several personal and business accounts at the filer's bank. Each of his cash deposits was split among his bank accounts in amounts ranging between $9,000 and $10,000. He also deposited numerous money orders that

were apparently purchased by several different individuals, though handwriting similarities noted in the signatures on the money orders suggested they were all signed by the same individual. The filer of the key SAR also reportedly suspected the defendant of check kiting based on the number of the defendant's personal checks drawn on other financial institutions and returned unpaid to the filer bank as the bank of first deposit.

Another SAR filed by this bank in 2006 revealed the defendant's continued pattern of structuring cash deposits. Further information gleaned from the bank revealed the defendant's purchase of large cashier's checks, some of which were payable to individuals with no known business affiliation to him.

During the course of the investigation, federal law enforcement officials were unable to determine the source of the bulk of the cash the defendant deposited. However, agents suspect that the money came from drug trafficking, currency smuggling, and/or questionable real estate dealings. Two additional SARs report the defendant's possible involvement in mortgage loan fraud. The defendant's attorney maintained that the defendant saved the bulk of the structured cash over time, storing it in his home for the proverbial rainy day.

At sentencing, the federal judge suggested that the defendant's structuring activity strongly pointed to some type of related criminal activity. The defendant pleaded guilty to the structuring charges and received a sentence that included home detention, probation, and a fine.

Section 4 - Issues & Guidance

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

Date of "Initial Detection" and the 30-Day SAR Clock

By FinCEN Office of Outreach Resources

Bank Secrecy Act suspicious activity reporting rules require that a SAR be filed no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR .[6] Upon identification of unusual activity, additional research is typically conducted and institutions may need to review customer transaction or account activity to determine whether to file a SAR. The need to review a customer's account activity, including transactions, does not necessarily indicate the need to file a SAR, even if a reasonable review of the activity or transaction might take an extended period of time. The time period for filing a SAR starts when the institution, in the course of its review or as a result of other factors, reaches the conclusion that it knows, or has reason to suspect, that the activity or transactions under review meets one or more definitions of suspicious activity.

Guidance on the timing of when a SAR must be filed was first set forth in the October 2000 *SAR Activity Review: Tips, Trends & Issues (Issue 1)*.[7] In May of 2006, FinCEN issued additional guidance in *The SAR Activity Review: Tips, Trends & Issues*

6. If no suspect can be identified, the time frame for filing a SAR is extended to 60 days.
7. SAR Activity Review: Trends, Tips, & Issues: Issue 1: http://www.fincen.gov/news_room/rp/files/sar_tti_01.pdf

(Issue 10)[8] to clarify any ambiguity in the interpretation of the original guidance. Institutions continue to seek clarification about the phrase "initial detection", and so FinCEN is issuing additional guidance with examples that illustrate appropriate timing for filing a SAR.

As clarified in the May 2006 *SAR Activity Review: Tips, Trends & Issues (Issue 10)*, the phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an accountholder's normal account activity. A real estate investment (purchase or sale), or the receipt of an inheritance or gift, for example, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. An institution's automated account monitoring system or initial discovery of activity, such as system-generated reports, may flag the transaction for review; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulations.

Institutions may have implemented multi-layer review procedures and/or systems in order to better detect and report suspicious activity. FinCEN recognizes that these multi-layer review processes may involve such steps as a red flag notice from an account monitoring system, a brief review by an analyst, and an investigation by an investigator. For example, an institution may have implemented an automated red flag system that detects unusual patterns in transactions. It may then utilize an analyst as a first step in determining whether the red flag notice is an obvious "false positive" or whether the activity should be forwarded to an investigator. In this example, the analyst makes no formal determination as to whether the activity may be suspicious based on the unusual transaction pattern and instead refers the matter to an investigator. After a period of appropriate review, the investigator determines whether the activity is suspicious. Thus, the date of initial detection is the date when the investigator has appropriately reviewed the activity and makes a determination that it is suspicious, not when the analyst refers the matter to the investigator.

The following examples illustrate that the date of initial detection does not necessarily occur on the date of the transaction(s), the date when an automated system generates a notice or red flag alert, or the date when an employee initially

8. SAR Activity Review: Trends, Tips, & Issues: Issue 10:: http://www.fincen.gov/news_room/rp/files/sar_tti_10.pdf

reviews the transaction(s). The following examples assume that the monetary thresholds have been met per the SAR regulation applicable to the specific type of institution. Note: Institutions are reminded that reviews of suspicious activity should be completed in a reasonable period of time.[9]

Examples:

Example 1: A customer makes two deposits of $9,900 over the course of two business days. On the third day, an alert teller notifies the BSA analyst that the customer has made deposits of just below $10,000 two days in a row. The analyst makes a determination that the two deposits of $9,900 are most likely indicative of structuring and therefore, the transactions are suspicious. That same day, the analyst refers the matter to the investigator and notes that the transactions are suspicious and likely involve intent to structure transactions to avoid CTR reporting requirements. The date of initial detection in this example is the date when the analyst was able to make a determination that the activity is suspicious. The institution has 30 days to file a SAR from the date of the analyst's determination.

Example 2: An import/export business customer suddenly begins sending and receiving large wire transfers from high risk jurisdictions. The institution's automated account monitoring system generates a red flag notification to the BSA officer, who conducts an initial review of the transactions. Given the complexity of the customer's business, the BSA officer is not in a position to determine whether the transactions may be suspicious. The officer refers the information to the institution's SAR investigator, who spends several days reviewing the customer's transactions and researching the nature of the customer's import/export business. After ten days of research, the investigator is able to make a determination that the activity does not appear to have a business or lawful purpose, and, therefore, the activity is suspicious. The day on which the investigator makes such a determination should be considered the date of the initial detection, and the institution has 30 days from that date to file a SAR.

---

9. According to the section "Timing of a SAR Filing" from the FFIEC Bank Secrecy Act/Anti-Money Laundering Manual (2007), "What constitutes a reasonable period of time will vary according to the facts and circumstances of the particular matter being reviewed and the effectiveness of the SAR monitoring, reporting, and decision-making process of each bank. The key factor is that a bank has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed." http://www.ffiec.gov/bsa_aml_infobase/default.htm

Example 3: An individual purchases money orders at several agent locations of an institution within the same city on the same business day. The next day, the institution's software system alerts the BSA assistant to the pattern of transactions. The assistant reviews the transactions and determines that transactions should be reviewed by the institution's BSA officer. The officer commences a review and a few days later the officer identifies another series of transactions conducted by the individual but still does not have enough information to determine if the activity is suspicious. A week later, the individual initiates a wire transfer to a high risk jurisdiction and provides the agent's employee with alarming information during a conversation. The employee informs the BSA officer of the updated information, and the officer makes a determination that the activity is suspicious, that a SAR should be filed, and that law enforcement should be contacted immediately. From that date, the institution has 30 days to file a SAR.

Section 5 - Industry Forum

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into some aspect of compliance management or fraud prevention that present their view of how they implement the BSA within their institutions. The Industry Forum section provides an opportunity for the industry to share its views. The information provided may not represent the official position of the U.S. Government.

Implementation of FACT Act May Warrant Further Analysis of ID Theft by FinCEN

By John Byrne, Bank of America

One of the key issues facing law enforcement and the financial industry is the critical obligation to report identity theft activities in a prompt and efficient manner. While this reporting requirement has been with the industry for some time, the issuance of final rules under The Fair and Accurate Credit Transactions Act of 2003[10] (the "FACT Act") necessitates that each financial institution have in place by November 1, 2008 an "Identity Theft Prevention program" to, among other things, identify, detect and respond to relevant "red flags." This is a brief overview of the red flags, as well as a request for FinCEN to provide new analysis of SAR filings to assist the industry with this reporting obligation.

In June, 2001, FinCEN highlighted the trend of identity theft and reminded the public of the laws in place, specifically "the *Identity Theft and Assumption Deterrence Act of 1998*" which amended 18 USC § 1028 to make it a federal crime for anyone to:

10. The FACT Act expanded the Fair Credit Reporting Act and is intended primarily to help fight identity fraud. The Act contains a number of provisions to help reduce identity theft, such as fraud alerts for victims of identity theft, and active duty alerts for persons in the military, making fraudulent applications for credit more difficult. The Act addresses accuracy and privacy of information, limits on information sharing, and consumer rights to disclosure, and requires secure disposal of consumer information.

knowingly [transfer] or [use], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.[11]

FinCEN also reviewed SAR narratives at the time that showed the most common ways to become the victim of identity theft are through the loss or theft of a purse or wallet, mail theft, and fraudulent address changes.

FACT Act Identity Theft Red Flags

The financial industry now has the obligation to establish policies and procedures in a program designed to formally address identity theft. While most institutions were already reporting activities that were determined to evidence identity theft, the FACT Act final rules demand both a response to red flags and a process to update the program when there are changes in identity theft risk. The rules reference sources of red flags as actual incidents of identity theft, the methods a bank has identified that reflect changes to identity theft risk, and supervisory guidance. The following are examples of regulatory "Red Flags":

Consumer Report Indicators

- A fraud or active duty alert is included with a consumer report.
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
  - A recent and significant increase in the volume of inquiries;
  - An unusual number of recently established credit relationships;
  - A material change in the use of credit, especially with respect to recently established credit relationships; or
  - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

11. The FTC defines Identity Theft as "fraud that is committed or attempted using a person's identifying information without authority."

Suspicious Documents

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

- Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
  - The address does not match any address in the consumer report; or
  - The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  - The address on an application is the same as the address provided on a fraudulent application; or
  - The phone number on an application is the same as the number provided on a fraudulent application.

- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  - The address on an application is fictitious, a mail drop, or a prison; or
  - The phone number is invalid, or is associated with a pager or answering service.
- The SSN provided is the same as that submitted by other persons opening an account or other customers.
- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
- The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
- For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

- Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:
  - The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
  - The customer fails to make the first payment or makes an initial payment but no subsequent payments.

- A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
  - Nonpayment when there is no history of late or missed payments;
  - A material increase in the use of available credit;
  - A material change in purchasing or spending patterns;
  - A material change in electronic fund transfer patterns in connection with a deposit account; or
  - A material change in telephone call patterns in connection with a cellular phone account.
- A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
- Mail sent to the customer is returned repeatedly as undeliverable, although transactions continue to be conducted in connection with the customer's covered account.
- The financial institution or creditor is notified that the customer is not receiving paper account statements.
- The financial institution or creditor is notified of unauthorized charges of transactions in connection with a customer's covered account.

Note: FinCEN acknowledges that the issue of identity theft continues to be a concern for financial institutions, and agrees with the recommendation to undertake a review of SAR filings in this area with a goal towards publishing an advanced analytic product in the future.

Section 6 - Feedback Form

Financial Crimes Enforcement Network
U.S. Department of the Treasury

Your feedback is important and will assist us in planning future issues of The SAR Activity Review. Please take the time to complete this form. The form can be faxed to FinCEN at (202) 354-6411 or accessed and completed online at http://www.fincen.gov/feedback/fb.sar.artti.php. Any questions can be submitted to sar.review@fincen.gov. 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

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

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

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

__ **Insurance Company**
__ **Dealers in Precious Metals, Precious Stones or Jewels**
__**Other** (please identify): _____

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

	1=Not Useful, 5=Very Useful				
Section 1 - Director's Forum	1	2	3	4	5
Section 2 - Trends and Analysis	1	2	3	4	5
Section 3 - Law Enforcement Cases	1	2	3	4	5
Section 4 - Issues & Guidance	1	2	3	4	5
Section 5 - Industry Forum	1	2	3	4	5
Section 6 - Feedback Form	1	2	3	4	5

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

_____
_____
_____
_____

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

_____
_____
_____
_____

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

_____
_____
_____
_____

G. What questions does your financial institution have about *The SAR Activity Review* that need 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
[ ] October 2005	[ ] May 2006	[ ] May 2007	[ ] Oct 2007
[ ] May 2008			

Please fax Feedback Forms to:

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

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

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