The SAR Activity Review

Trends Tips & Issues

Issue 20

Published under the auspices of the BSA Advisory Group.
October 2011

Financial Crimes Enforcement Network

The SAR Activity Review

Trends Tips & Issues

Issue 20

Published under the auspices of the BSA Advisory Group.
October 2011

Table of Contents

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

Introduction

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

This issue of *The SAR Activity Review* covers a wide range of topics. The *Trends & Analysis* section features articles by two of FinCEN's multi-disciplinary working groups: SAR filings related to international prepaid cards, and the risks associated with the growth in Remote Deposit Capture (RDC) services. FinCEN's Office of Regulatory Analysis shares findings of their assessment of SAR filings prior to and following FinCEN's Advisory on Informal Value Transfer Systems (IVTS) in September, 2010. Also, FinCEN's Office of Outreach Resources provides an update on SAR-related inquiries to our Regulatory Helpline.

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

In *Issues & Guidance*, we present articles from the United States Trustees Program on their efforts in combating bankruptcy-related mortgage fraud and mortgage rescue schemes and from Immigration and Customs Enforcement (ICE) on organized retail crime. We also include several articles from FinCEN staff focusing on a variety of topics of interest for financial institutions: health care fraud and associated red flags; SAR confidentiality; distinguishing between BSA SARs and other suspicious activity reporting initiatives; and, E-filing information for filers of the Registration of Money Services Business form (FinCEN Form 107). We also include in this section an update to FinCEN's February, 2011 Advisory on Elder Financial Exploitation.

Finally, in the *Industry Forum*, we get an industry viewpoint on the money laundering risks associated with trading cash for gold.

You can subscribe to FinCEN Updates under "What's New" on the FinCEN website, www.fincen.gov, to receive notification of when *The SAR Activity Review – Trends, Tips & Issues* is published. As always, we very much appreciate your feedback. Please take a moment to fill in the form in Section 6 to let us know if the topics we have covered are helpful to you, as well as what you would like to see covered in future editions. The form may be forwarded to FinCEN at the email address sar.review@fincen.gov. Please do not submit questions regarding suspicious activity reports to *The SAR Activity Review* mailbox.

Barbara Bishop
Regulatory Outreach Project Officer
Financial Crimes Enforcement Network

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

Helene Schroeder
Special Counsel
Commodity Futures Trading Commission

Michael Cho
Global Head, Anti-Money Laundering Compliance
Northern Trust

Section 1 — Director's Forum

During the April 2000 meeting of the Bank Secrecy Act Advisory Group (BSAAG), the suggestion was made to "*Develop a report to provide regular feedback on current trends, patterns and methodologies noted in SARs, along with guidance on policy issues affecting the industry…*" That suggestion, from one of our financial industry partners, has resulted in this ongoing publication and has contributed to our continuing efforts, in coordination with the financial industry, to provide as much guidance and feedback about the utility of Suspicious Activity Reports (SARs) as our resources allow.

Much has changed since then, but the continued relevance of the articles and commentary found in *The SAR Activity Review – Trends, Tips & Issues* has only grown. The breadth and depth of available SAR data has greatly expanded. FinCEN's main sources of SAR information continue to include almost 15,000 banks and credit unions, almost 45,000 Money Services Businesses, and about 900 casinos. The banks and credit unions alone occupy over 100,000 offices and branches located in every corner of America. The USA PATRIOT Act's AML authorities brought other financial industries under FinCEN SAR regulations; over 7,000 mutual funds, over 1,000 insurance companies, and thousands of securities or commodities brokerage firms. FinCEN continues to expand its responsibilities and available sources of SAR information. Our most recent final rule, Definitions and Other Regulations Relating to Prepaid Access affects thousands of businesses, and addresses the money laundering threat that prepaid cards, internet transfers, mobile payments, and other prepaid devices may pose.

FinCEN's small staff of approximately 300 professionals is of necessity, and by design, organized to most efficiently collect, protect, share, and analyze FinCEN's SAR information. Our regulatory experts, with diverse industry expertise, craft complex rules. Our law enforcement liaisons facilitate and protectively monitor the flow of information between the industry and criminal investigators. FinCEN's technical experts are designing the next generation of information systems to help

better interpret and share the vast amount of information we hold in the public trust. And, across divisions, we have analysts who work daily with domestic and international financial data to develop useful intelligence. The synergies among FinCEN's divisions, and our constant interaction with the financial industry through vehicles like our regulatory helpline, allow us to spot trends, to discover issues, and to provide the rich and deep feedback you will find in this *Review*.

Two-way communication with the financial industry is critical to what we do. Some of the issues we together face are just emerging, like the incipient risks presented by Remote Deposit Capture (RDC), and the red-hot cash-for-gold markets that have recently flourished. You will find comprehensive articles exploring those risks inside this *Review*. Other issues demand continued long term vigilance, like the long-recognized money laundering threat inherent to Informal Value Transfer Systems (IVTS), often referred to as *Hawala*. FinCEN since its inception has been reporting on and sharing its information about IVTS and several *SAR Activity Review* articles and case examples have been previously published. This *Review* takes a thorough, quantitative look at how FinCEN guidance and IVTS red flag indicators positively impact industry SAR filings.

Through our *Outreach Initiatives*, FinCEN has proactively and systematically arranged face-to-face meetings between our leadership and staff with a variety of financial institutions both large and small. The information and the industry insight that we, as a regulator, have gained from these meetings has been remarkable. Of special note, one of the recurring issues raised as part of our meetings with smaller community banks was the topic of elder financial exploitation. The care and concern that these bankers exhibited for their most vulnerable customers led directly to FinCEN's elder financial exploitation advisory. An examination of the SAR activity resulting from that advisory is included herein. We hope this feedback will provide additional insights on how banks can protect their customers from criminal abuse.

Communication *between* financial institutions is also one of the keys to effectively managing money laundering and fraud risks, and can help institutions to protect themselves as well as their peer businesses and customers. Section 314(b) of the USA PATRIOT Act allows, and FinCEN has been encouraging, just such information sharing. One of the case examples we present shows how a 314(b) call between bankers, combined with bank SARs, and casino CTRs led to a guilty plea by a Ponzi scheme operator.

Also within, you will find illuminating articles on the importance of FinCEN information in our joint efforts with law enforcement and the financial industry to combat mortgage fraud, healthcare fraud, and organized retail crime. On behalf of FinCEN's staff and our partner contributors, I welcome you to this exceptionally informative issue of *The SAR Activity Review*.

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

Section 2 — Trends & Analysis

This section of *The SAR Activity Review – Trends, Tips & Issues* contains information on BSA filing trends and SAR-related calls received by FinCEN's Regulatory Helpline.

Analysis of International Prepaid Card-Related SAR Filings

By FinCEN Staff[1]

Background

The prepaid card industry originated when companies began replacing paper gift certificates with magnetic stripe-bearing gift cards based on existing credit and Automated Teller Machine (ATM) or debit card models. Over time, prepaid cards gained broad acceptance as their accessibility and capabilities have expanded. These capabilities include the ability to deposit additional funds by reloading the card, withdraw cash from an ATM, transfer funds between users, and pay bills. The ease of obtaining prepaid cards and their potential anonymous use make prepaid access products attractive to consumers but also may make them vulnerable to illicit activity. Internationally capable prepaid cards with large-dollar cash withdrawal functionality raise the most consistent concern for U.S. law enforcement.[2]

This article provides an interim assessment of financial institutions reporting on the misuse of international prepaid cards, issued either by a U.S. or non-U.S. institution. FinCEN will publish a comprehensive report on this subject later this year.

1. A special multi-disciplinary working group of FinCEN analysts, regulatory outreach specialists, public affairs specialists, special agents, and information technology personnel contributed to this article.
2. See Financial Action Task Force, "Money Laundering Using New Payment Methods," October 2010 (http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf).

Regulatory Overview

Until recently, FinCEN had regulated "stored value" to a lesser degree than other forms of money services business (MSB) activity, in part to allow the fledgling industry to develop. Since that time, what we now refer to as "prepaid access" has become increasingly prevalent in American commerce. In an effort to establish a more comprehensive regulatory regime for an industry whose technological advances have outpaced existing rules, FinCEN recently promulgated new requirements for prepaid access on July 26, 2011.[3] FinCEN will continue to follow the further evolution of the prepaid access industry and review the need for possible future rulemakings to help ensure the effective application of existing regulations.

Methodology

For the purposes of this article, the term "prepaid card" refers to payment cards that are funded in advance of use at a certain monetary value. This analysis does not use the term "prepaid" or "prepaid access" as FinCEN defined that term in its Prepaid Access Final Rule. FinCEN analysts completed keyword searches in the narratives and "Other" field of SARs filed by all types of financial institutions for indications of international prepaid card activity. From that research, FinCEN analysts identified 3,090 international prepaid card SARs. The study then selected a random sample of 793 SARs for purposes of evaluating SAR narratives discussed in this assessment. This sample size enabled a confidence level of 95 percent and confidence interval of +/-3 percent.[4]

Preliminary Findings

Based upon a review of the entire population of identified international prepaid card SARs filed during the period from January 1, 2008, through June 30, 2011, FinCEN identified a number of important preliminary findings:

3. Definitions and Other Regulations Relating to Prepaid Access, 76 FR 45403 (July 26, 2011).

4. The randomly selected sample included 626 depository institution SAR, 152 Suspicious Activity Report by Money Services Business (SAR-MSB), and 15 Suspicious Activity Report by the Securities and Futures Industries (SAR-SF) filings. The sample did not include the one Suspicious Activity Report by Casinos and Card Clubs (SAR-C) filing, but an analyst reviewed it independently to inform the overall analysis. The sample selection percentages mirrored those of the broader population of identified international prepaid card filings.

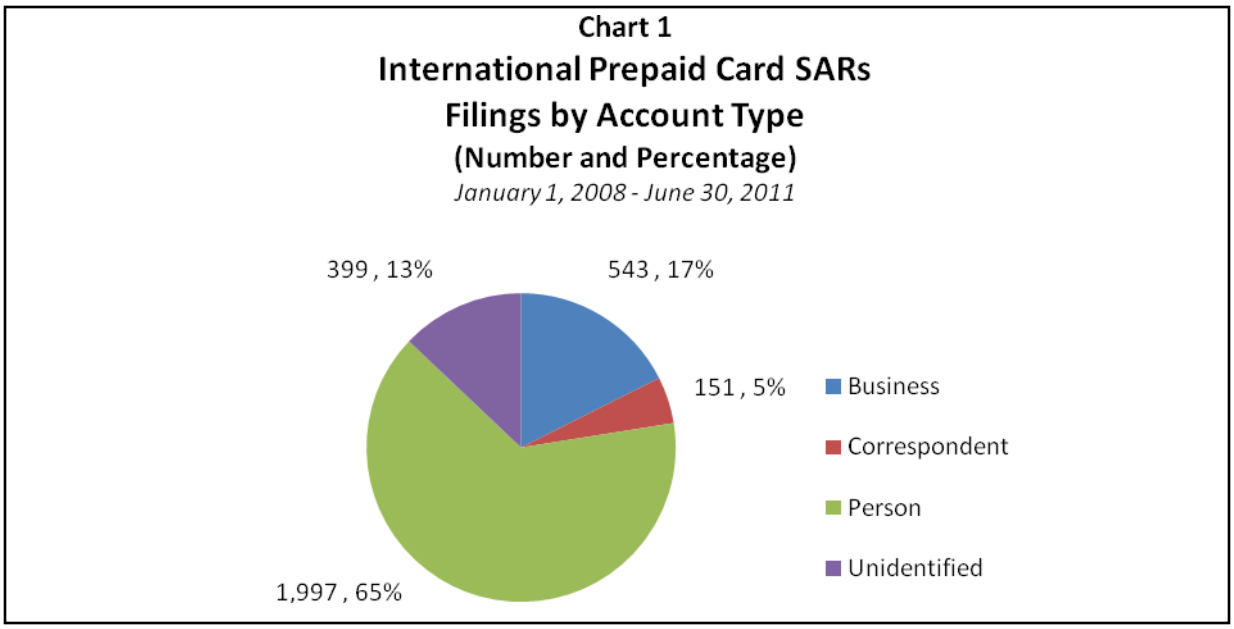
International prepaid card SARs represented a miniscule percentage of all SAR filings during the study period.

Compared to all the SARs filed during the same three and a half year period, those that reported an international prepaid card connection represented less than one-tenth of a percent of the total (0.07%) and accounted for less than two-tenths percent (0.19%) of the suspicious activity amount reported.[5] Banks filed by far the largest share (2,456 or 79 percent) of SARs related to international prepaid card transactions.

Financial institutions primarily identified suspicious activity involving accounts held by individuals rather than businesses or other financial institutions.

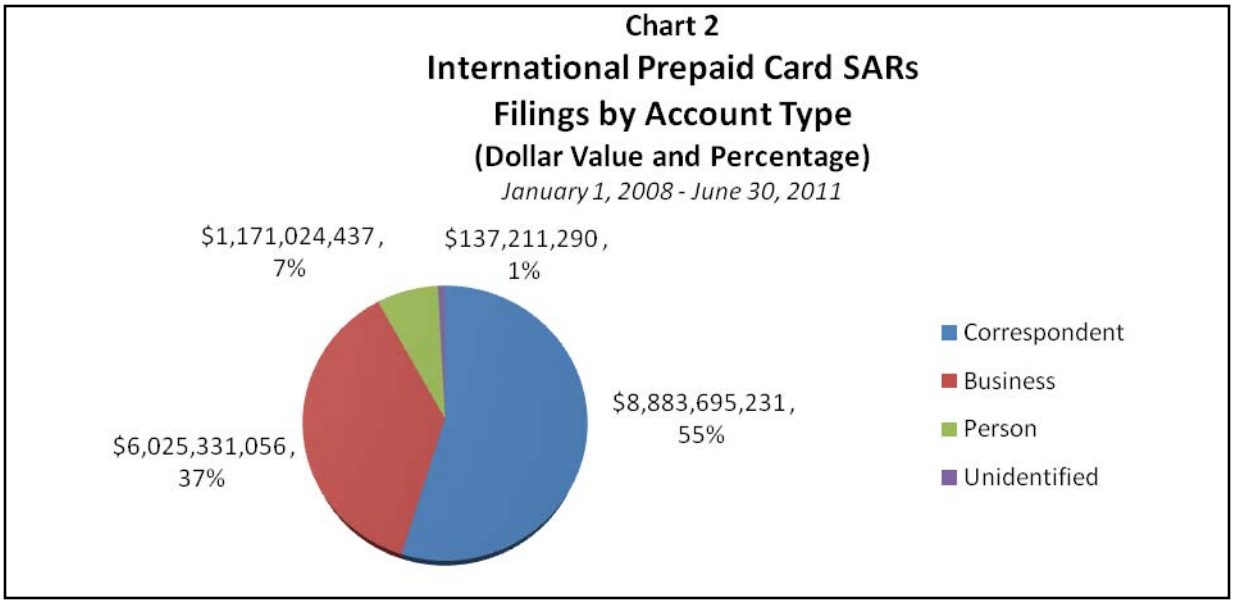
Approximately two-thirds of all international prepaid card SAR filings identified an individual account as the source of the suspicious activity. This focus would appear directly related to the filing financial institutions' greater ability to identify transactional outliers at the individual cardholder or transactional customer level. FinCEN's new regulations, which extend SAR filing requirements to non-bank providers and sellers of prepaid access, should further aid in identifying suspicious international prepaid card transactions conducted by individuals.

5. For a comparison with other recent international-related SAR studies, please see the May 2011issue of The SAR Activity Review – Trends, Tips & Issues, and the "Assessment of Remote Deposit Capture (RDC) Risks" article within this publication.



The vast majority of the total dollar amount of international prepaid card activity associated with SAR filings involved a correspondent banking account relationship or business.

Banks pointed to their correspondent banking relationship channels for the majority of the dollar value associated with all international prepaid card SARs. These filings generally involved particularly large numbers of transactions. Indication of the involvement of a business account came from banks as well as securities and futures industries SAR filers.



International prepaid card SAR filings were global in scope, but the majority of SAR references involved just sixteen countries.

Analysts identified 181 foreign jurisdictions, with some filings including references to multiple foreign jurisdictions. Sixteen foreign jurisdictions accounted for a majority of the 5,458 total SAR filing references (see Table 1).

Table 1

International Prepaid Card SARs Filed by Banks References to Non-U.S. Jurisdictions January 1, 2008 – June 30, 2011		
Jurisdiction Name	***References***	***Cumulative Percentage***
UNITED KINGDOM	539	10%
CANADA	306	15%
JAMAICA	300	21%
MEXICO	220	25%
UNITED ARAB EMIRATES	193	29%
CHINA	159	31%
GERMANY	135	34%
PHILIPPINES	125	36%
PANAMA	124	38%
INDIA	117	41%
VENEZUELA	117	43%
HONG KONG	105	45%
CYPRUS	98	47%
RUSSIA	97	48%
CAYMAN ISLANDS	93	50%
NIGERIA	87	52%
OTHER JURISDICTIONS	2,643	100%

Banks

Based upon the randomly selected bank SAR filings, it appears that filers often listed international prepaid card activity as a secondary rather than the primary reason for considering the underlying transactional activity suspicious. Filers commonly cited suspected money laundering or structuring activity, "Other" suspicious activity, identity theft, and credit card fraud.

A particularly notable element among the identified bank filings involved the use of ATMs located outside of the United States to make large withdrawals of currency, sometimes during short, concentrated windows of time. Five hundred twenty-two, or 21 percent, of bank SARs noted suspicious ATM withdrawals ranging from $155 to cumulative transactions totaling greater than $20.5 million; 18 of these filings involved amounts, when aggregated, of greater than $1 million. Such filings underscore the potentially elevated risk associated with prepaid cards that support international ATM cash withdrawal access, a key element of the risk-based approach of FinCEN's recent prepaid access final rule.

MSBs

MSBs filed 584 SARs related to international prepaid card usage; only one was related to a business, but it did not include any suspicious activity amount. The filer determined that the business acted as an MSB check casher agent (allegedly without an appropriate state license) and a seller of money orders and prepaid cards. After reviewing the narrative section of the remaining 583 reports, analysts attributed all the other SAR-MSBs to an individual's personal account relationships and determined the suspicious activity amount aggregated to $16.3 million. The most frequently cited basis for reporting MSB suspicious activity was account takeover, followed by transactions involving identified high-risk jurisdictions.

Securities and Futures

Securities broker-dealers and commodities futures merchants filed 49 SARs related to international prepaid card activity. The filings only indicated activity associated with individual's personal account relationships or business' account relationships. As with other filings, money laundering or structuring was the initial description of the suspicious activity implicating international prepaid card activity. Unlike other filings, however, SAR-SF filers reported identity theft as the single largest category (excluding the general "Other" category). Among the examples that prompted filings: breaches of prepaid card processors' payment systems; initiation of trades and debit card purchases of prepaid cards from new trading accounts before funds to open or augment the account were settled; and liquidation of mutual funds (at least in part to fund prepaid cards) in transactions involving high-risk jurisdictions and suspect customer identification information.

Casinos/Card Clubs

The single SAR-C associated with international prepaid cards reported that a guest staying at a casino hotel purchased $7000 worth of gift cards with cash, reportedly for convenience, before returning home to another country.

Common Typologies Related to Suspicious International Prepaid Card Activities

A review of 793 randomly selected SARs filed by banks, MSBs, and securities and futures firms identified withdrawals at ATMs located in foreign countries, transactions with foreign Web sites, and international wire transfers as the main suspicious activities involving the use of international prepaid cards outside the United States. Financial institutions deemed the activities suspicious based on the size, frequency, and nature of the transactions as well as the jurisdictions and types of financial vehicles used. Banks reported most of these activities.

An important element of the suspicious international prepaid card activity discussed in these typologies is the use of prepaid cards within the layering or integration stages of traditional money laundering.[6] After initially removing the illegal proceeds from the source accounts, especially through account takeovers or identity theft, the subjects eventually purchased prepaid cards for resale or with international cash withdrawal capabilities. FinCEN's preliminary review of these filings appears to demonstrate the appropriateness of FinCEN's risk-based approach in the recent final rule to international and cash withdrawal prepaid access capabilities. This preliminary review also indicates these filings appear to be generally consistent with a number of law enforcement concerns related to international prepaid card transactions.

A forthcoming report on international prepaid card transactions will explore these and other identified typologies in detail.

6. Money laundering can be a complex process. It involves three different, and sometimes overlapping, stages. Placement involves placing illegally obtained money into the financial system or the retail economy. Money is most vulnerable to detection and seizure during placement. Layering involves separating the illegally obtained money from its criminal source by layering it through a series of financial transactions , which makes it difficult to trace the money back to its original source. Integration involves moving the proceeds into a seemingly legitimate form. Integration may include the purchase of automobiles, businesses, real estate, or prepaid cards.

Assessment of Remote Deposit Capture (RDC) Risks

By FinCEN Staff[7]

Background

Remote Deposit Capture (RDC) is a rapidly growing service that an increasing number of banks are providing to business customers and, in some cases, individual customers. RDC services allow customers to remotely deposit electronic check images to their accounts, creating a new channel for traditional deposit collection activities. These services are a direct outgrowth of the Check Clearing for the 21st Century Act or Check 21 (PL 108-100), which has facilitated the greater use of electronics within the check collection system.[8]

The potential and actual risks associated with RDC have been highlighted within recent supervisory guidance, particularly the 2010 FFIEC Exam Manual[9] and 2009 FFIEC Guidance on RDC Risk Management,[10] as well as within FinCEN's RDC-related enforcement actions.[11] These risks are of increasing interest given the nearly ubiquitous use of Check 21 authority to collect checks electronically between banks as well as the growing percentage of checks deposited electronically with the bank of first deposit.[12]

Recent Enforcement Actions

In March 2010 and February 2011, FinCEN assessed civil money penalties against two banks for violations pertaining to RDC. These penalties highlight the potential risks associated with the initial adoption of new technologies or use of those technologies to provide innovative products and services. Significantly, the

---

7. A special multi-disciplinary working group from FinCEN's Regulatory Policy and Programs Division and Analysis and Liaison Division contributed to this article.
8. See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ100.108.pdf.
9. See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf#page=210.
10. See http://www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf.
11. See http://www.fincen.gov/news_room/ea/files/100316095447.pdf and http://www.fincen.gov/news_room/nr/pdf/20110211.pdf.
12. See http://www.federalreserve.gov/newsevents/press/other/20101208a.htm.

penalized banks were early adopters of electronic check image technology that provided RDC services beyond their traditional customer base. The cases contained common elements from which other banks contemplating the provision of RDC services or their expansion to broader customer bases may gain important lessons:

- failure to identify and assess the compliance and operational risks associated with RDC prior to implementation;
- inadequate internal controls necessary to manage the additional anti-money laundering (AML) risks posed by RDC activity, and insufficient resources for the monitoring of RDC transaction activity;
- utilization of RDC for processing certain deposit items from non-United States correspondent accounts, in particular casa de cambio (CDC) accounts; and
- insufficient automated transaction monitoring systems that permitted suspicious activity associated with RDC to go undetected and unreported for lengthy periods of time.

Methodology

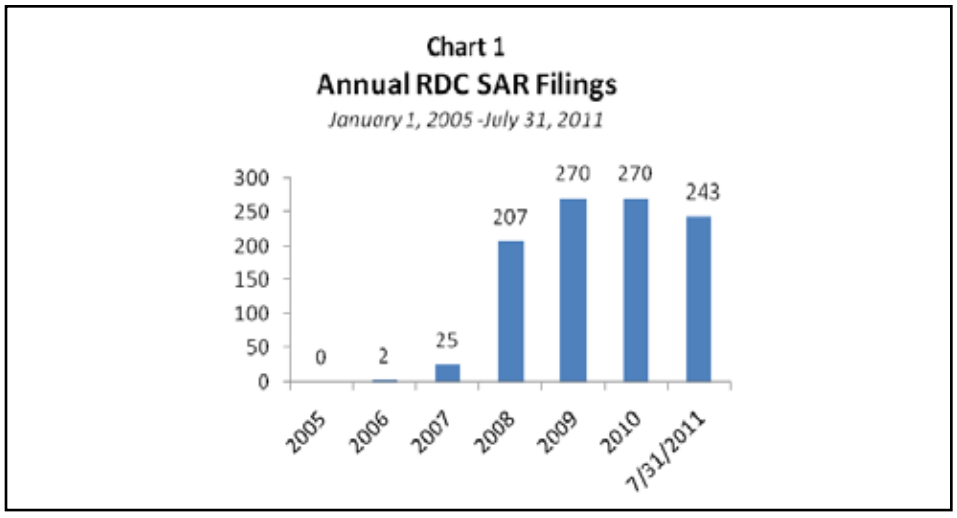
The remainder of this assessment describes suspicious activities relating to the use of RDC services as reported by financial institutions to FinCEN between January 1, 2005, and July 31, 2011. FinCEN analysts identified the relevant SARs through a search for relevant keywords within the narratives of the depository institution SAR, Suspicious Activity Report by the Securities and Futures Industries (SAR-SF), and Suspicious Activity Report by Money Services Businesses (SAR-MSBs) filings. Because SAR-SF and SAR-MSB reports were de minimus and RDC services are almost exclusively bank deposit services, this assessment focuses solely on information gained from bank SAR filings.

FinCEN analysts identified 1,017 SAR filings associated with RDC. After reviewing these SARs in their entirety, analysts categorized the filings on an annual basis into the following suspicious activity characterization fields identified by filers as indicative of check fraud: Category A – BSA/Structuring/Money Laundering; Category C – Check Fraud; Category D – Check Kiting, and Category H – Counterfeit Check. A large percentage of SARs (41 percent) listed MSBs/CDCs as subjects of the reported suspicious activity. Analysts compared these filings with those which listed other businesses or individuals as subjects, which this report refers to as miscellaneous subjects, to identify trends, patterns and examples of activities. FinCEN analysts also researched media and industry reports and law enforcement activities related to the misuse of RDC services.

General Filing Trends

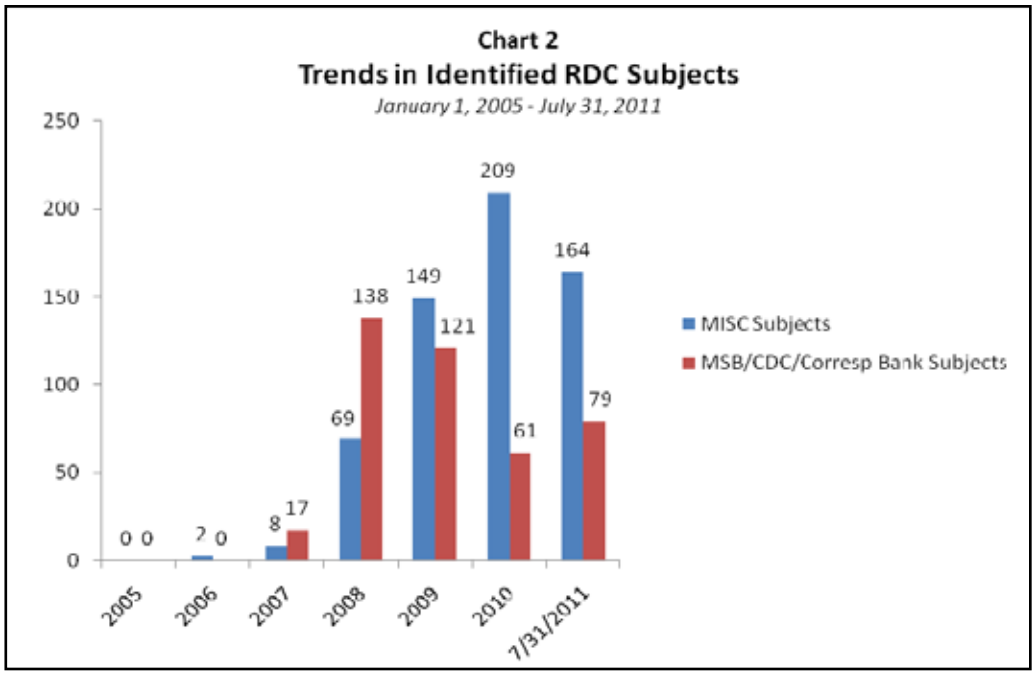
RDC-related SAR filings have been minimal, but are increasing over time, possibly as a result of assessments of civil money penalties.

Overall, RDC-related filings constituted approximately 0.1 percent of all bank SARs related to check fraud, check kiting, and counterfeit checks filed during the review period. As noted in Chart 1, the increase in filings generally tracked with the timing of the previously noted assessments of civil money penalties. FinCEN analysts found a noticeable increase in RDC-related SAR filings in 2011 following the issuance of the civil money penalties. The major check fraud activities also constituted about 39 percent of the total RDC-related filings across the entire study period, with the remaining 61 percent identified as related to general Bank Secrecy Act (BSA) and money laundering activities.



MSBs/CDCs have been the most common identifiable subjects among RDC-related bank SAR filings.

The general trend in SAR filings associated with MSBs/CDCs was related to FinCEN's assessments of civil money penalties in 2010 and early 2011 (see Chart 2). Two banks accounted for approximately one-third of all the MSB/CDC-related SAR filings. Analysts also found an increase in these filings in 2011 that appears to reflect the growing number and types of banks offering RDC services to broader customer bases. While miscellaneous subjects have become more common, there were no significant commonalities among the industries represented. The increase in miscellaneous subjects appeared to be in part related to the general weakness of U.S. business conditions, with a number of filings indicating that businesses used RDC services to fraudulently enhance funds availability to cover immediate business expenses (check kiting).

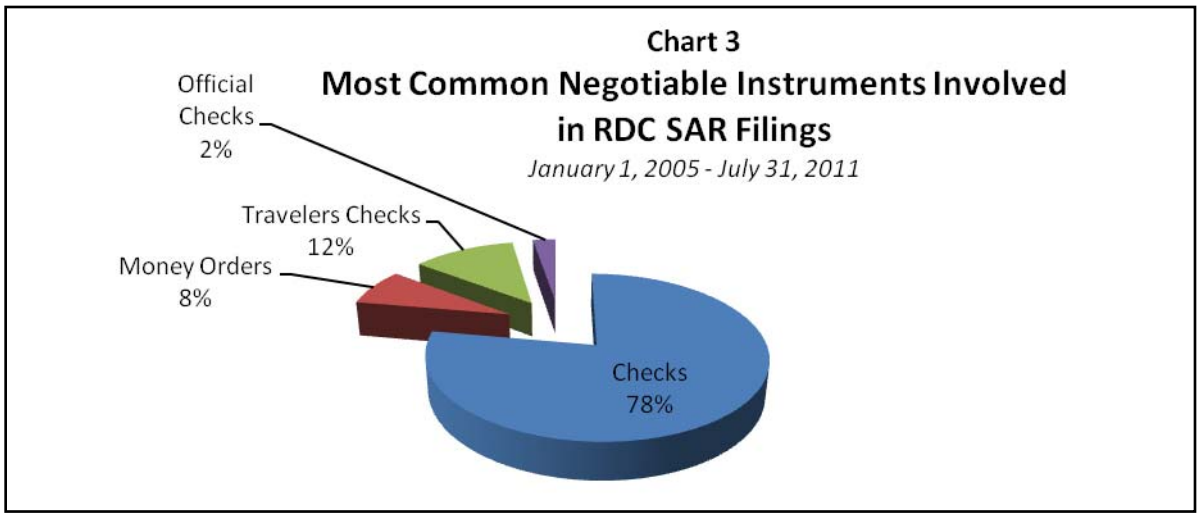


International transactions were common.

As highlighted within the assessments of civil money penalties and underscored from industry feedback, RDC is increasingly being used to replace traditional check collection practices, such as pouch mailings. SAR filers described activities by CDCs from Mexico and MSBs from other countries, such as the Dominican Republic, Ecuador, Guatemala, South Korea, Israel, Panama, and Trinidad & Tobago, as using RDC services to deposit checks to correspondent, general business, or personal accounts within the United States.

While checks were the most common instrument identified in RDC-related SAR filings, the use of traveler's checks and money orders was common in MSB/CDC-related filings.

As noted in Chart 3, the vast majority of RDC-related SAR filers associated suspicious activities with the deposit of third-party or personal checks. This mix of negotiable instruments is consistent with expectations for deposits made by MSBs, specifically check cashers. Additionally, some filings associated with MSBs noted the suspicious deposit of sequential or incomplete money orders.



Typologies

Overall, our review of bank SAR filings indicated no real differences in the various fraud and money laundering schemes perpetrated through the RDC check deposit channel when compared with check deposits completed through more traditional means. RDC-related SAR filings regularly identified check kiting, counterfeit or altered checks, and other common check fraud schemes. At most, the choice of the RDC deposit channel may have facilitated certain schemes or the expansion of services to non-traditional customers somewhat more effectively than traditional check deposit channels. The following describes some schemes reported in SAR narratives by type of subject.

U.S. and Foreign-Located MSBs

Banks filed SARs on both U.S. and foreign-located MSBs. In some cases, banks filed SARs on the customers of these MSBs rather than the MSBs themselves.

Foreign MSBs

A limited number of banks filed hundreds of SARs on certain foreign-located MSBs. One foreign-located MSB had relationships with numerous U.S. banks with which it deposited checks via RDC. The MSB would then wire the funds to a bank in its own country through a U.S. correspondent. Banks also reported MSBs depositing third-party checks with missing data and sequentially ordered money orders or traveler's checks. In other instances, institutions reported on the activities of MSB customers of their correspondent banks. These activities were sometimes detected during routine cash letter reviews. Some filers reported offering RDC services directly to MSBs or CDCs located outside the United States from which the suspicious activity emanated.

Customers of U.S.-located MSBs

Banks also reported on the activities of the customers of U.S.-located MSBs to which they offered RDC services. These included structured check cashing or presentment of sequentially numbered checks. Some filing banks reported offering RDC services to MSBs located in other geographic regions.

Instruments

Within the MSB/CDC filings, banks typically noted that the deposited negotiable instruments included third-party checks, sequentially numbered money orders, and traveler's checks. Structured cash withdrawals or outgoing wires sometimes followed these deposits.

Miscellaneous Individuals and Businesses

For most of the study period, commercial banks filed the majority of miscellaneous subject SARs; in 2011, however, credit unions contributed an increasing number of filings as more began making RDC services available. The occupations of these subjects varied widely, and the activity involved no common business type. The identified activities also were generally consistent with traditional check fraud schemes.

Double Presentment of Checks

Banks reported instances where paper checks already deposited electronically using RDC services were presented again for deposit in a teller line. Conversely, banks reported cases where checks that had already been negotiated were presented again for deposit via RDC. While fraudulent check re-presentment schemes are not new, the use of RDC services did provide an additional channel for their perpetration. This potential risk was recognized during the creation of Check 21, leading to the inclusion of expedited consumer re-credit provisions and a system of warranty and liabilities.

Counterfeit/Altered Checks

Banks reported the use of RDC to present counterfeit checks; checks which were altered; checks which bore false routing or MICR numbers; and checks with forged or missing endorsements. Suspicious activity also included the deposit of checks payable to third parties. In some cases, the customer depositing the check was the apparent perpetrator; in other instances, the customer was the victim of apparent advance fee schemes. Banks also reported altered checks drawn on U.S. Department of the Treasury or state treasuries. Numerous filers became aware of the activity upon return of the checks for non-sufficient funds (NSF), or altered, stop payment and counterfeit notifications.

Transfers, Withdrawals, and Purchases

Suspicious activity involving RDC was often accompanied by immediate attempts to transfer or access the credited funds. Banks noted subjects conducting multiple transfers between accounts they owned at the same or other banks, including transfers between business and personal accounts. In some cases, the suspicious activity also included incoming wire transfers from domestic or foreign banks. Deposits of checks that would later be returned as NSF or counterfeit were often followed by structured cash withdrawals or by point of sale purchases with the credit or debit cards.

Check Kiting

As noted earlier, some subjects attempted to take advantage of check float times to enhance funds availability within their business accounts. In some of these instances, the filer did not mark the suspicious activity characterization of "check kiting," but described such activity in the narrative.

International Cash Letter

Certain filers noted suspicious activity conducted by the customers of their correspondent banks in various countries. These customers deposited sequentially numbered checks, which the correspondents presented to the filer via RDC. In these cases, the clients of the correspondent did not appear to be MSBs.

Conclusions

While the adoption of RDC technologies may pose additional challenges to financial institutions, particularly banks, the industry's related SAR filings comprise a miniscule portion of all check-fraud related bank SARs. We expect, however, that RDC-related SAR filings could increase as more institutions offer the service to broader customer bases. Filings also may increase as the lessons learned from recent enforcement actions are incorporated into existing anti-money laundering policies, procedures, and systems. The increased number of RDC filings through the first half of 2011 appears to reflect both of these trends. Additionally, we found that the typologies associated with RDC-related SAR filings generally mirrored those of traditional paper check fraud.

The adoption of new technologies or use of those technologies to provide innovative banking products and services, such as RDC services, also raise additional risk management considerations. As the recent enforcement actions demonstrate,

even larger institutions have experienced a learning curve when broadly offering RDC services; smaller commercial banks and credit unions may require additional guidance to identify and appropriately mitigate these risks. In some cases, special precautions and commensurate due diligence efforts may be appropriate when processing items from non-U.S. correspondent accounts or foreign-located customers. Banks may wish to perform periodic reviews of and generate risk management reports on the AML issues associated with RDC. Banks also may wish to ensure that their transaction monitoring systems adequately capture, monitor and report on suspicious activities occurring through RDC, especially as transactional levels increase.

An Analysis of SARs Related to Informal Value Transfer Systems Filed Before and After FinCEN's September 2010 Advisory

By FinCEN's Office of Regulatory Analysis

On September 1, 2010, FinCEN published an advisory concerning Informal Value Transfer Systems (IVTS). The advisory reminded financial institutions of previously published IVTS information, and requested that filers include the abbreviation "IVTS" in the narrative section of Suspicious Activity Report (SAR) filings so that SARs referencing IVTS can be more helpful to law enforcement.[13]

This article aims to assess the effectiveness of the advisory by comparing pre- and post-advisory SAR filing trends and patterns. It analyzes depository institution SARs filed from November 1, 2009 through June 30, 2011 that contain the term IVTS in their narratives.[14]

13. FinCEN, *Informal Value Transfer Systems, FinCEN Advisory FIN-2010-A011*, 1 September 2010 at http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2010-A011.pdf and FinCEN, *Informal Value Transfer Systems, FinCEN Advisory 33*, March 2003 at http://www.fincen.gov/news_room/rp/advisory/pdf/advis33.pdf

14. This study analyzed only SARs submitted by depository institutions, which accounted for nearly all SARs containing references to IVTS in their narratives.

IVTS Background

FinCEN's advisory defined IVTS as any system, mechanism, or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form. Transactions generally take place outside the conventional banking system. Expatriates and immigrants often use IVTS to send funds to friends and family in their home countries. Companies that conduct business in countries without a formal financial system also use IVTS.

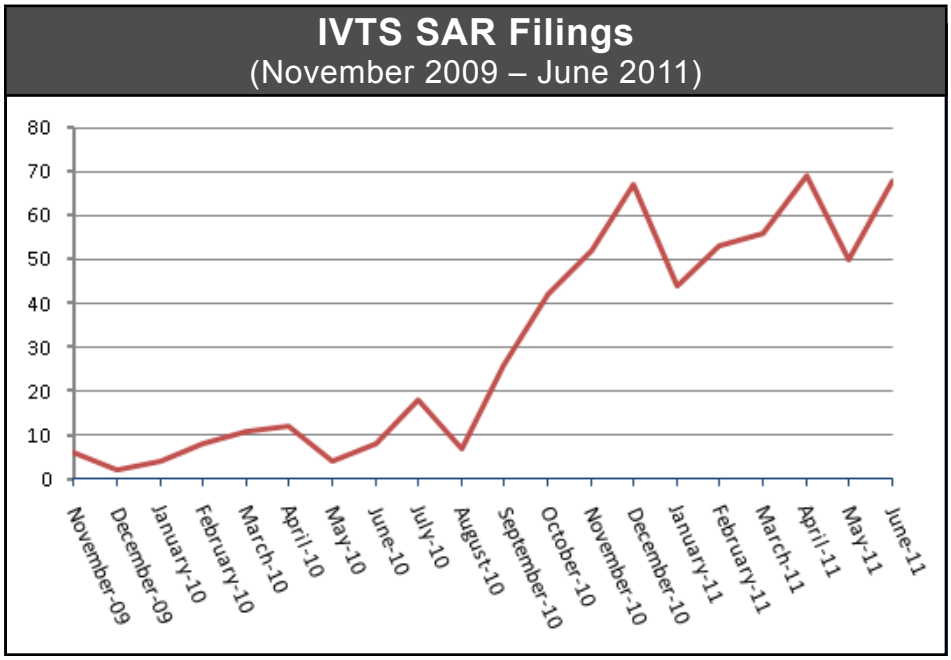
Due to their versatility and anonymity, IVTS are vulnerable to misuse. Criminals may use IVTS to launder proceeds from illicit activities. Reports also indicate possible use of IVTS to fund attempted terrorist attacks, including attacks against the United States.

IVTS SAR Filings

SAR filings containing the term IVTS in the narrative increased by 559 percent after FinCEN published the advisory. FinCEN analysts identified 80 such SARs filed in the 10 months prior to the advisory and 527 SARs filed in the 10 months afterwards. Filers referenced the FinCEN advisory in 21 percent of post-advisory SAR filings.[15]

15. 111 SARs referenced the FinCEN advisory. Some filers referred to the advisory as FinCEN guidance. These filings were included in the total.

Graph 1[16]



Filing Institutions

Forty six unique institutions filed SARs containing the term IVTS during the 20 months before and after publication of the advisory. The top three filers, responsible for 40 percent of post-advisory SARs, did not file any "IVTS SARs" prior to the Advisory. Table 1 indicates that all but 4 of the top 15 filers included the term IVTS after the Advisory was published.

16. Increases in SAR filings are not necessarily indicative of an overall increase in IVTS-related activities because financial institutions may have previously reported IVTS-related suspicious activity without including the term IVTS.

Table 1

SAR Filings Containing IVTS in Narrative Top 15 SAR Filers (November 2009 - June 2011)						
	Pre-Advisory		***Post-Advisory***		***Total Filings***	
Top Filer	***SARs***	***% of 80***	***SARs***	***% of 527***	***SARs***	***% of 607***
A	0	0	91	17%	91	15%
B	0	0	76	14%	76	13%
C	0	0	72	14%	72	12%
D	19	24%	27	5%	46	8%
E	2	3%	40	8%	42	7%
F	0	0	41	8%	41	7%
G	0	0	33	6%	33	5%
H	2	3%	23	4%	25	4%
I	17	21%	7	1%	24	4%
J	0	0	22	4%	22	4%
K	13	16%	7	1%	20	3%
L	17	21%	0	0	17	3%
M	0	0	16	3%	16	3%
N	0	0	8	2%	8	1%
O	0	0	7	1%	7	1%

Some top filers consistently quoted the "FinCEN Advisory," recited IVTS suspicious activity criteria, and/or described how the subjects met the IVTS criteria. Many filers regularly requested supporting documentation to verify potential IVTS transactions; advised clients that unregistered IVTS activity was illegal and should be stopped; monitored accounts every 90 days; set up alerts on unregistered IVTS operators; and, closed accounts. Filers also cited previous related filings that did not reference IVTS.

Trends and Patterns in IVTS SAR Filings

- The majority of all SAR filings during the study period contained descriptions of suspicious currency exchange activity. Before the advisory, filers primarily described currency exchange activities in Latin American countries. After the advisory, filers continued to report suspicious currency exchange activities in Latin America as well as suspicious Middle Eastern transactions, most involving the United Arab Emirates (UAE), Yemen, and Iran.
- Filers referenced unregistered and/or unlicensed money services business (MSB) related activity in 30 percent of all relevant SARs, 92 percent of which were post-advisory filings.
- Filers consistently described suspicious activities that were indicative of both money laundering[17] and IVTS. Filers selected the "Bank Secrecy Act/ Structuring/Money Laundering" characterization of suspicious activity in 79 percent of SARs and used the "Other" field in 53 percent of SARs to describe IVTS and other MSB related activities.
- Filers described suspicious activities conducted by 2,481 subjects, 51 percent with domestic addresses, 41 percent with foreign addresses, and 8 percent not associated with any addresses. Almost 40 percent of foreign addresses were located in Venezuela, while the majority of domestic subjects had addresses in New York and California.

17. Money laundering can be a complex process. It involves three different, and sometimes overlapping, stages: Placement involves placing illegally obtained money into the financial system or the retail economy. Money is most vulnerable to detection and seizure during placement. Layering involves separating the illegally obtained money from its criminal source by layering it through a series of financial transactions, which makes it difficult to trace the money back to its original source. Integration involves moving the proceeds into a seemingly legitimate form. Integration may include the purchase of automobiles, businesses, real estate, etc.

Currency Exchange

The majority[18] of IVTS SAR filings contained descriptions of suspicious currency exchange activity, apparently intended to avoid currency exchange restrictions/ controls and/or save money on fees. Filers described the following types of currency exchange activity:

- Customers used exchange houses that instructed them to transmit funds through an unknown third party (IVTS operator) to receive currency in another country.
- Customers utilized family and friends' accounts or related business accounts to perform currency exchange.
- Entities used business accounts to conduct currency exchange for known and unknown individuals. Filers generally reported that system alerts detected pass-through activity in accounts involving unknown entities.

Almost half of the IVTS SAR filings (47 percent) referenced suspicious activity involving currency exchange in Latin American countries.

Table 2

IVTS SAR Filings
Top Suspicious Currency Exchange Activity Locations
(November 2009 - June 2011)

	Pre-Advisory		*Post-Advisory*		*Total Filings*	
Countries	***SARs***	***% of 80***	***SARs***	***% of 527***	***SARs***	***% of 607***
Venezuela	32	40%	160	30%	192	32%
Argentina	24	30%	36	7%	60	10%
Brazil	13	16%	11	2%	24	4%
Mexico	2	3%	10	2%	12	2%
Total	**71**	**89%**	**217**	**41%**	**288**	**48%**

18. Approximately 57 percent of IVTS SAR filings contained descriptions of suspicious currency exchange activity.

Venezuela

Almost a third (32 percent) of the IVTS SARs reported currency exchange activities relating to Venezuela. According to filers, Venezuelans utilized illegal parallel currency exchange mechanisms to circumvent currency exchange controls implemented by the Venezuelan government in 2003 to prevent capital flight.[19] In addition, numerous SARs referenced suspicious activity involving securities and the Venezuelan parallel market.[20]

Argentina

About a tenth of the SARs reported currency exchange transactions related to Argentina, involving the use of exchange houses that instructed customers to transmit funds through unknown third parties in Uruguay and Panama to receive local currency.

Whereas 89 percent of pre-advisory SARs reported suspicious currency exchange activity in Latin American countries, just 41 percent of post-advisory SARs did so. Meanwhile, the proportion of post-advisory SARs describing activity occurring in the Middle East increased.

Middle East Transactions

Filers described the following types of suspicious transactions involving accounts held in the Middle East: third party transactions conducted through exchange houses in Jordan, Kuwait, and the UAE; high volumes of wires through Middle Eastern correspondents' accounts; and apparent unregistered MSB activity involving checks and wires to the Middle East. Suspicious currency exchange-related activity involved suspicious checks and wires to Yemen (7 percent) and the use of UAE exchanges and trading companies by Iranians residing in the United States (8 percent). All Yemen- and Iran-related SARs were filed post-advisory.

19. See U.S. Department of State, *2011 Investment Climate Statement – Venezuela*, March 2011 at http://www.state.gov/e/eeb/rls/othr/ics/2011/157383.htm

20. In June 2010, Venezuela created a new and legal parallel foreign exchange market, essentially a currency exchange market that operates through bond swaps. See U.S. Department of State, *2011 Investment Climate Statement – Venezuela*, March 2011 at http://www.state.gov/e/eeb/rls/othr/ics/2011/157383.htm

Yemen

Depository institutions submitted 42 post-advisory SARs referencing Yemen. Filers described "unknown but organized money movements" and suspected that customer accounts facilitated money transmission between the United States and the Middle East. In over half (52 percent) of Yemen-related SARs, filers reported potential unregistered MSB activities. Filers suspected IVTS operations based on suspicious cash deposits and checks involving Yemen often conducted through convenience/grocery store accounts. Common check characteristics included: sequential check numbers, the application of stamped symbols or notes in Arabic on checks, and handwriting variations. Numerous SARs referencing "Yemen ICL" listed the names of Yemeni correspondent banks and described checks negotiated in the Middle East through international cash letters (ICL).[21] Filers referenced the FinCEN advisory in 40 percent of Yemen-related SARs.

Iran

Filers referenced IVTS transactions potentially involving Iran in 49 SARs (8 percent), all filed post-advisory. Filers commonly described remittances from family members in Iran (43 percent) to Iranians residing in the United States. Almost 70 percent of Iran-related SARs involved transactions through the UAE, trading companies (37 percent), and/or MSBs. In 37 percent of SARs, customers allegedly stated the transactions either resulted from the sale of property in Iran or were intended for U.S. real estate purchases, renovations, or mortgages. Filers referenced the FinCEN advisory in 57 percent of Iran-related SARs.

Unlicensed / Unregistered MSBs[22]

Overall, filers submitted 181 SARs (30 percent) describing unlicensed and/or unregistered MSB activities, of which 47 percent referenced unlicensed/unregistered currency exchange. Most significantly, filers submitted 92 percent of the SAR filings post-advisory. Most pre-advisory SARs described "unregistered money transmissions," while half of post-advisory SARs included references to "unlicensed currency exchange."

---

21. In basic terms, an international cash letter is an inter-bank transmittal letter that accompanies checks or monetary instruments (such as money orders) sent from one bank to another internationally. For information on ICL vulnerabilities, see *The SAR Activity Review: Trends, Tips & Issues*, Issue 6, pages 18-20, November 2003 at http://www.fincen.gov/news_room/rp/files/sar_tti_06.pdf

22. Filers variously used the terms unregistered and unlicensed to describe MSBs that failed to register with FinCEN, to receive the appropriate state licenses, and/or maintain appropriate state registration(s).

Most filings referenced unregistered/unlicensed individuals or businesses (i.e. exchange houses in the Middle East and Latin America, or domestic/foreign businesses) that utilized personal or business accounts to conduct MSB-related transactions. Filer descriptions of suspicious activity involving domestic unregistered MSB subjects generally involved suspicious cash deposits from unknown persons followed by checks issued to overseas beneficiaries or funds transferred through U.S. registered MSBs to overseas beneficiaries. Filers suspected that overseas beneficiaries might act as IVTS to disburse funds to unknown "true" beneficiaries. Filers frequently indicated the subjects were not registered with FinCEN.

Table 3 relates filer descriptions of unlicensed/unregistered MSB-related suspicious activity.

Table 3

IVTS SAR Filings
Types of Unlicensed/Unregistered MSB Activity Reported[23]
(November 2009 - June 2011)

	Pre-Advisory		*Post-Advisory*		*Total MSB-related Filings*		*Total IVTS Filings*
	SARs	***% of 15***	***SARs***	***% of 166***	***SARs***	***% of 181***	***% of 607***
Currency Exchange	2	13%	83	50%	85	47%	14%
Money Transmission	8	53%	41	25%	49	27%	8%
Prepaid Access[24]	0	0%	8	5%	8	4%	1%
Check Casher	0	0%	2	1%	2	1%	0%

23. Filers used various terms to describe unlicensed/unregistered suspicious activities (i.e. money service business vs. money services business, currency exchange vs. currency FX.) The table grouped similar terms.

24. Filers' descriptions of possible unregistered MSB activity relating to prepaid access included a) receiving money transfers and checks referencing the purchase of phone/calling cards, and b) entities that allegedly stated they sold or expected to sell phone cards. According to one filer, this activity appeared IVTS-related because its customer acted as a middle man for calling card purchases that the bank customer's customer could have purchased directly from the supplier.

Subject Locations[25]

The 607 IVTS SARs named 2,481 subjects. Of these, about 25 percent were listed in both pre- and post-advisory filings. Over 40 percent (1,019 subjects) were associated with foreign addresses, almost 40 percent of them in Venezuela. About 81 percent (828) of the foreign subjects were associated with addresses in the top 10 countries noted in Table 4.

Table 4

IVTS SAR Filings Top 10 Subject Countries (November 2009 - June 2011)		
Country	***SARs***	***%***[26]
Venezuela	397	39%
Argentina	85	8%
Mexico	74	7%
UAE	53	5%
Brazil	51	5%
Panama	49	5%
Uruguay	36	4%
Hong Kong	30	3%
Afghanistan	28	3%
Virgin Islands	25	2%
Total	**828**	

New York (37 percent) and California (24 percent) lead as the top locations of the 1,256 domestic subjects. Over 90 percent of New York filings reporting possible unregistered MSB activity involved transactions between convenience/grocery store accounts and the Middle East.

25. Filers did not include addresses for 8 percent of reported subjects.

26. Some SARs listed multiple subjects from varying overseas locations.

Reported Suspicious Activity

Narrative analysis indicated filers reported suspicious account activities indicative of money laundering and IVTS. In addition to regularly reporting transactions involving unknown originators and beneficiaries, filers consistently reported the following suspicious activities.

Table 5

IVTS SAR Filings **Reported Potential Suspicious Activity Associated with Money Laundering**[27] (November 2009 - June 2011)						
	Pre-Advisory		***Post-Advisory***		***Total Filings***	
	SARs	***% of 80***	***SARs***	***% of 527***	***SARs***	***% of 607***
Even/Round/Whole Dollar Amounts	8	10%	126	24%	134	22%
High Risk Jurisdiction	11	14%	96	18%	107	18%
No Business Purpose	14	18%	70	13%	84	14%
Unknown Source of Funds	8	10%	73	14%	81	13%
Structuring	14	18%	52	10%	66	11%
Pass Through	13	16%	30	6%	43	7%
Layering	7	9%	33	6%	40	7%
Sequential Checks	3	4%	17	3%	20	3%

Analysis identified subtle narrative reporting differences between the pre- and post-advisory filings. For example, the number and percentage of SARs reporting suspicious transactions involving even, round, or whole dollar amounts increased significantly. Also, pre-advisory SARs that cited "high risk jurisdictions" primarily named Panama and Venezuela. In post-advisory SARs, many filers also named "high risk jurisdictions" in the Middle East, primarily the UAE, Iran, and Yemen.

27. Some SARs listed multiple types of suspicious activity.

Table 6 lists types of financial transactions frequently referenced in IVTS-related SARs, including transactions referencing "loans" and "invoices," involving friends and family members, and relating to the sale/purchase of real estate. A few filers also described activities they associated with potential trade based money laundering (TBML)[28] and Black Market Peso Exchange (BMPE).[29]

Table 6

IVTS SAR Filings Other Reported Suspicious Activity (November 2009 - June 2011)						
	Pre-Advisory		***Post-Advisory***		***Total Filings***	
	SARs	***% of 80***	***SARs***	***% of 527***	***SARs***	***% of 607***
Loans	9	11%	82	16%	91	15%
Family & Friends	7	9%	73	14%	80	13%
Real Estate Purchase/ Sale	12	15%	58	11%	70	12%
Invoices	4	5%	54	10%	58	10%
TBML	1	1%	18	3%	19	3%
BMPE	0	0%	15	3%	15	2%

Loans

A filer stated that international customers began calling IVTS transfers "loans" after learning that suspicious IVTS transactions could precipitate account closures. Filers reported references to "loan repayments" or "loans" in 15 percent of SARs. Filers consistently contacted customers regarding the alleged loans and learned they were often repayments of personal loans obtained to help with business and living expenses. Loan-related transactions involved:

- Unlicensed currency exchange under the guise of loans, commonly involving the exchange of Venezuelan for U.S. currency.

28. TBML is the illicit use of trade operations and related activities to disguise the proceeds of criminal activity through the use of trade transactions, including misrepresentation of the price, quantity and quality of imports or exports. See FinCEN, *Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering*, FinCEN Advisory FIN-2010-A001, 18 February 2010 at http://www.fincen.gov/statutes_regs/guidance/html/fin-2010-a001.html

29. The BMPE facilitates "swaps" of dollars, owned by the cartels, in the United States for pesos already in Colombia, by selling the dollars to Colombian businessmen who are seeking to buy United States goods for export. See FinCEN, *Black Market Peso Exchange Update, FinCEN Advisory, Issue 12*, June 1999 at http://www.fincen.gov/news_room/rp/advisory/pdf/advis12.pdf

- Customers' redirection of "loan repayments" to an unknown third party, who was supposedly borrowing money from the original lender.

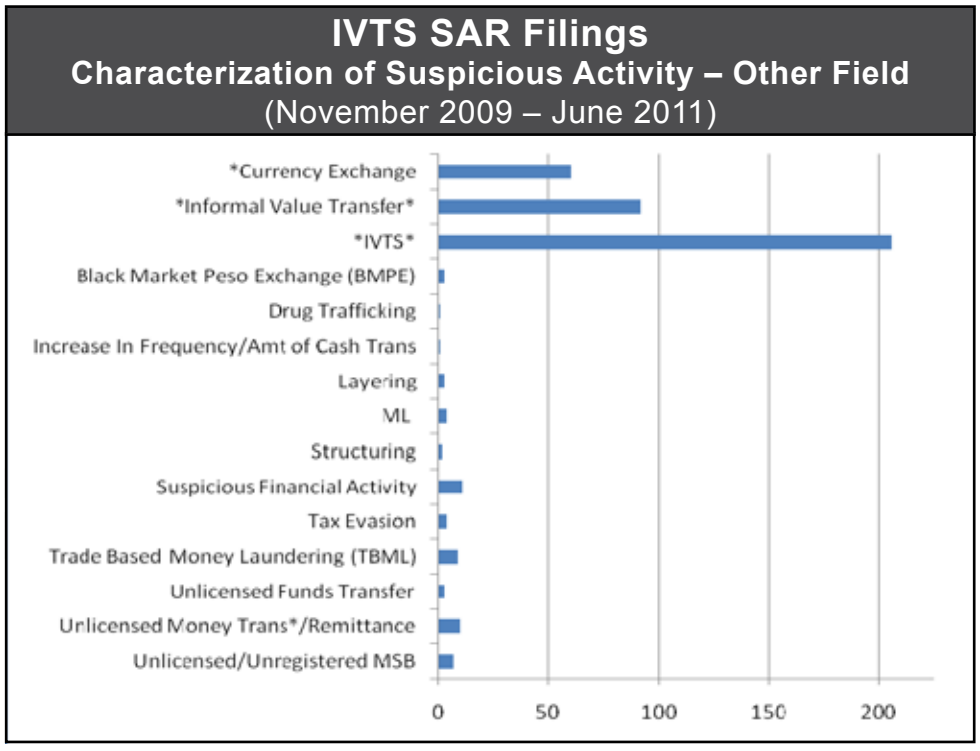
Invoices

All pre-advisory filings referencing invoices described invoices provided as supporting documentation for transactions. Post-advisory SAR filings also detailed discussions with customers regarding invoices and described invoice references on checks and in wires to indicate invoice payment.

Characterizations of Suspicious Activity

Filers selected the characterization of suspicious activity "BSA/Structuring/Money Laundering" in 79 percent of SARs and "Other" in 53 percent of SARs.[30] The most common "Other" field descriptions were IVTS, Informal Value Transfer, and Currency Exchange. There was no distinguishable difference between filings before or after the advisory.

Graph 2[31]



30. Filers often selected multiple characterizations of suspicious activity, making the total greater than 100 percent.

31. These figures are a tally of "Other" field descriptions of suspicious activity. Some other field descriptions included multiple types of suspicious activity (e.g. IVTS/BMPE); therefore, totals do not equal 100 percent.

Summary

The IVTS advisory published in September 2010 has had measurable effects. Depository institution SARs including the term "IVTS" in the narrative substantially increased (559 percent) in the 10 months after FinCEN published its IVTS advisory. Filers referenced the FinCEN advisory in 21 percent of post-advisory IVTS SAR filings, and some top filers quoted the advisory, recited IVTS suspicious activity criteria, and/or described how the subjects met the IVTS criteria. Post-advisory SAR filings revealed that filers cited more "high risk" countries associated with IVTS. Nine of the fifteen top filers post- advisory had not included the term "IVTS" in any filings during the corresponding time period preceding the advisory.

Analysis of SAR Inquiries Received by FinCEN's Regulatory Helpline

By FinCEN's Office of Outreach Resources

FinCEN operates a Regulatory Helpline that provides assistance for financial institutions seeking clarification of their obligations under the Bank Secrecy Act (BSA) and certain requirements under the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act.[32] This article analyzes the 1,564 inquiries regarding SAR requirements that the Regulatory Helpline received from July 1, 2010, through June 30, 2011.[33] The article also highlights helpful FinCEN guidance for the most frequently received inquiries, including guidance on additional steps a financial institution should take after filing a SAR and how to characterize suspicious activity.

Key Trends

Volume trends

During the twelve month period ending June 30, 2011, the Regulatory Helpline received 1,564 inquiries related to SAR requirements, a 7 percent increase compared with the previous twelve month period ending June 30, 2010. However, these

32. Financial institutions can contact FinCEN's Regulatory Helpline at 800-949-2732.

33. All information provided in this publication has been aggregated to ensure the confidentiality of individual inquiries. The determination of entity type is primarily based upon caller self-identification.

inquiries accounted for only 12 percent of all Regulatory Helpline inquires for the year; this is a noticeable decrease from the 18 percent they represented the previous year. This resulted from a significant increase in the number of non-SAR inquiries related to fraud schemes,[34] the transfer of FinCEN's regulations from 31 CFR Part 103 to 31 CFR Chapter X (Chapter X),[35] and FinCEN's Agent Request Initiative.[36]

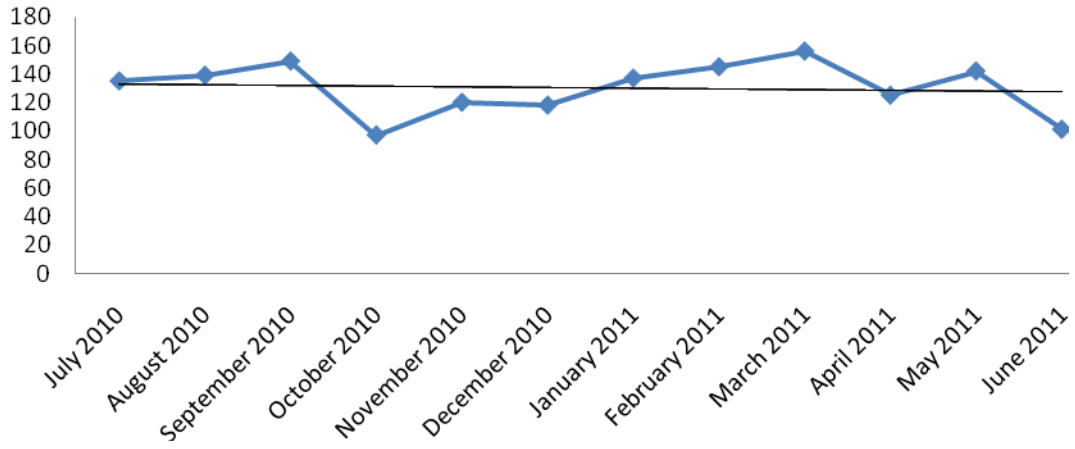
The most noticeable increase in SAR-related inquiries was associated with "other (SAR) regulation", which increased 450 percent (27 inquiries). These inquiries related to the final rule on "Confidentiality of Suspicious Activity Reports"[37] and the transfer of the SAR requirements to Chapter X. Additionally, inquiries related to understanding the rules for "sharing (SARs) with law enforcement" increased 36 percent (43 inquiries) compared with the previous year. This demonstrates continued industry interest in this topic; the October 2009 edition of *The SAR Activity Review – Trends, Tips & Issues* previously highlighted this issue and directed readers to earlier FinCEN guidance pieces.[38]

While general requests for "assistance with the SAR form" remained the most common type of inquiry (465 inquiries, or 30 percent of all SAR-related inquiries received), the number of inquiries decreased slightly from the previous year; this relative decline could reflect financial institutions' better overall understanding of the technical aspects of filing SARs. Regulatory Helpline calls also showed decreases in the volume of inquiries related to "characterizations of suspicious activity" (a 44 percent decrease) and "verification of SAR filings"[39] (38 percent decrease). All these trends could illustrate the accumulating benefit for financial institutions of *The SAR Activity Review* and FinCEN guidance.

---

34. See "FinCEN Reminds the Public to be Wary of Fraudulent Correspondence and Phone Calls," (http://www.fincen.gov/alert.html).
35. See "FinCEN's Streamlined Regulations in New Chapter X," (http://www.fincen.gov/news_room/nr/pdf/20110301.pdf).
36. See "FinCEN Asks MSBs to Provide Their List of Agents," (http://www.fincen.gov/news_room/nr/pdf/20110516.pdf).
37. See "FinCEN Rule Strengthens SAR Confidentiality," (http://www.fincen.gov/news_room/nr/pdf/20101122.pdf).
38. See *The SAR Activity Review - Trends Tips & Issues*, Issue 16 (http://www.fincen.gov/news_room/rp/files/sar_tti_16.pdf#page=30).
39. Financial institutions requested verification of receipt for SARs that were filed via paper.

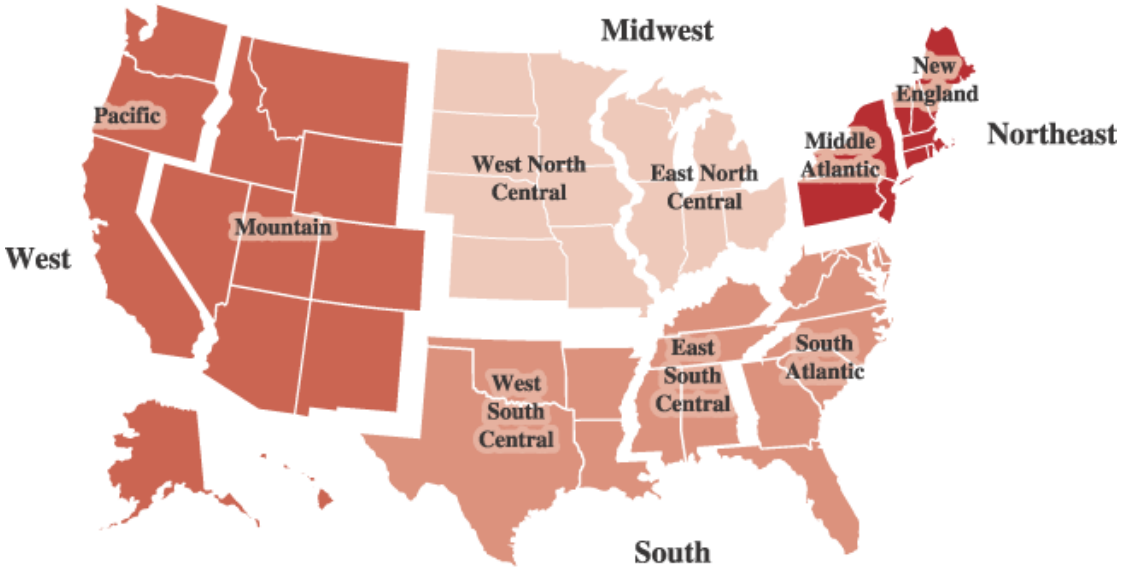
Financial Institution Inquiries Related to Suspicious Activity Reporting (SAR) Requirements (with overall trend line)
July 2010 to June 2011



Geographic Trends

The Regulatory Helpline received inquiries from all 50 U.S. states, as well as from the District of Colombia, Puerto Rico, the U.S. Virgin Islands, and Bermuda. Nine states, primarily California, Texas, New York, Florida, and Illinois, accounted for half of all the inquiries received during the study period; the previous year's analysis identified these same top five states. The regional dispersion of the inquiries also remained the same, with the highest concentration again coming from the South.

SAR Inquiries by Region
July 1, 2010 to June 30, 2011



WEST = 316	***NORTHEAST = 316***
Pacific = 228	New England = 106
Mountain = 88	Middle Atlantic = 210

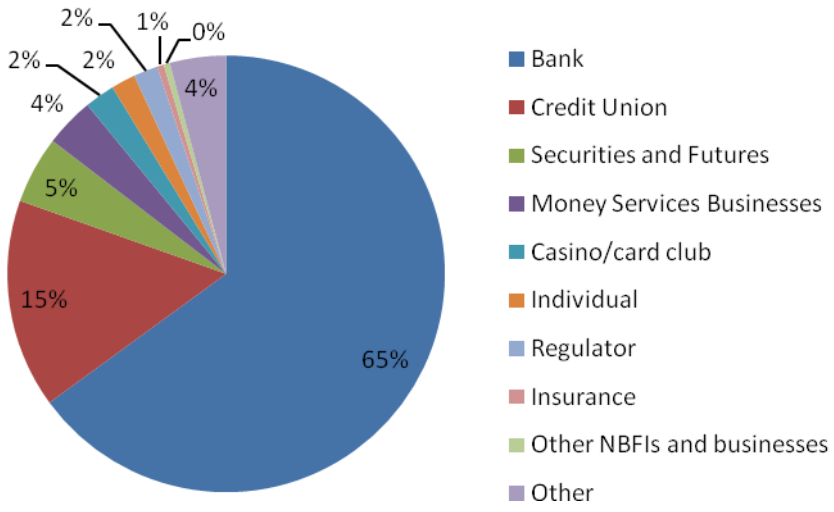
SOUTH = 518	***MIDWEST = 360***
West South Central = 199	West North Central = 166
East South Central = 68	East North Central = 194
South Atlantic = 251	

All Other = 54

There were some slight differences in the type of institutions that contacted the Regulatory Helpline across the four main regions of the country indicated above. Similar to the previous year's analysis, credit unions accounted for a higher percentage (24 percent) of all SAR-related inquiries from within the West Region, while averaging only 13 percent across the other three regions. Mirroring the overall increase, the number of SAR inquiries increased from the previous year's levels within each of the four regions.

Institution Type Trends

SAR Inquiries by Type of Financial Institution
July 1, 2010 to June 30, 2011



Bank[40]	1,018	Credit Union	242
Securities and Futures	78	MSBs[41]	57
Casino/card club	35	Individual	28
Regulator	28	Insurance	8
Other NBFIs and businesses[42]	5	Other	65
Total Requests	1,564		

40. This category includes banks, credit unions, savings & loans, and thrifts.
41. This category includes money transmitters; currency dealers and exchangers; check cashers (check cashers do not have a SAR filing obligation); issuers, sellers, and redeemers of traveler's checks, money orders, and stored value (transactions involving solely the issuance, sale, or redemption of stored value were not subject to a SAR filing obligation during this time period); and the United States Postal Service (for certain activities).
42. This category includes all other non-bank financial institutions and businesses, such as loan and finance companies, vehicle sellers, and dealers of precious metals, stones or jewels.

Key Issues and Themes

Identification of Key Issues and Themes
July 1, 2010 - June 30, 2011

Assistance with SAR Form	**465**
SAR item instructions	280
Form corrections	86
SAR narrative	38
Aggregation	32
Filing deadline	17
Deletion or rescission of a filed SAR	12
SAR Sharing and Disclosure	**355**
Sharing - Law Enforcement	161
Replying to a subpoena	73
Other disclosure questions	61
Sharing - Regulators/Auditors	36
Sharing - Corporate Structure	24
Guidance on Whether to File a SAR	**293**
Whether to file a SAR	179
Regulation	70
Monetary thresholds	35
Guidance on attempted activity	9
SAR Filing on Continuing Activity	**118**
Aggregation	55
Frequency of SAR Filings	30
Whether to file a SAR	17
FinCEN guidance	12
Monetary thresholds	4
Additional Steps a Financial Institution Should Take	**53**
Notification of authority (e.g. FBI, DEA, etc.)	33
Guidance on whether to close an account	20
Verification of SAR Filing	**49**
Verification of filing	33
Obtaining copies of a SAR	16
Characterizations of Suspicious Activity	**29**
Definitions	29
E-Filing	**29**
Miscellaneous	15
SAR item instructions	14
Other	**173**
Miscellaneous	72
Regulation	33
General guidance	26
FinCEN guidance	22
Safe Harbor	14
The SAR Activity Review	6
Total Inquiries for July 1, 2010 to June 30, 2011	**1564**

General SAR Filing Assistance

As noted earlier, the most frequent type of inquiry received on the Regulatory Helpline related to "assistance with the SAR form." The SAR Narrative Guidance Package[43] provides answers to many questions related to completion of the SAR form. The Regulatory Helpline also receives frequent inquiries related to correcting prior reports for minor or insignificant errors. FinCEN issued guidance in a previous edition of *The SAR Activity Review* that addressed Insignificant Suspicious Activity Report Filing Errors.[44] Additionally, FinCEN recently published the SAR filing specifications for the new FinCEN SAR that will be available for submission through the BSA E-Filing System beginning December 2011.[45]

Inquiries related to "SAR sharing and disclosure" were increasingly common, accounting for nearly one in every four SAR inquiries. To aid institutions in responding to law enforcement and regulatory authorities' requests for SAR information and supporting documentation, FinCEN issued guidance in June 2007 entitled, Suspicious Activity Report Supporting Documentation (FIN-2007-G003). Guidance on Providing Suspicious Activity Reports to Appropriate Law Enforcement is available in a previous edition of *The SAR Activity Review*.[46]

Inquiries related to "guidance on whether to file a SAR" accounted for about one in every five SAR inquiries. To assist in making this internal decision, institutions may refer to resources such as the FFIEC BSA/AML Examination Manual, Suspicious Activity Reporting Overview, SAR Decision-Making Process.

Highlighted below are other recent common inquiries to the Regulatory Helpline and associated helpful guidance.

Account Closure

Institutions frequently seek the guidance of FinCEN's Regulatory Helpline regarding potential additional steps to take after filing a SAR. One of the most common inquiries relates to whether an account should be closed after a certain number of SARs is filed on a customer.

---

43. See SAR Narrative Guidance Package (http://www.fincen.gov/statutes_regs/guidance/pdf/narrativeguidance_webintro.pdf).
44. See *The SAR Activity Review - Trends Tips & Issues*, Issue 9, Section 4 (http://www.fincen.gov/news_room/rp/files/sar_tti_09.pdf#page=48).
45. http://www.fincen.gov/news_room/nr/pdf/20110902.pdf
46. See *The SAR Activity Review - Trends Tips & Issues*, Issue 9 Section 5 (http://www.fincen.gov/news_room/rp/files/sar_tti_09.pdf#page=49).

The decision to maintain or close an account should be made by a financial institution in accordance with its own standards and guidelines. Institutions can find pertinent FinCEN guidance published in October 2000 in *The SAR Activity Review Issue 1, Section 5* under the topic of "Cessation of Relationship/Closure of Account."[47] In addition, institutions also can refer to FinCEN guidance (FIN-2007-G002) published in June 2007, Requests by Law Enforcement for Financial Institutions to Maintain Accounts.

Verification of SAR Filing

Institutions will occasionally contact the FinCEN Regulatory Helpline to verify the receipt, or request a copy, of a SAR filing. Financial institutions must maintain a copy of any SAR they file and the original or business record equivalent of any supporting documentation for five years from the filing date.[48]

Due to the confidentiality of these reports, FinCEN is unable to verify the receipt of, or provide a copy of, SAR filings. However, users of FinCEN's BSA E-Filing System[49] do receive SAR Acknowledgements[50] for BSA E-Filing submissions. While financial institutions cannot access their submitted SAR filings directly through the BSA E-Filing System, they must save their filings to their computer or network drives before the SARs can even be submitted. This E-Filing process greatly assists institutions in meeting their recordkeeping requirements. Institutions that utilize the BSA E-Filing System also should save their SAR filing acknowledgements and other notices. Certain other filing information will remain available to institutions within the BSA E-Filing System for up to 5 years. For more information about the benefits of BSA E-Filing, please review our helpful brochure.[51]

47. See *The SAR Activity Review, Trends Tips & Issues*, Issue 1 Section 5 (http://www.fincen.gov/news_room/rp/files/sar_tti_01.pdf)
48. The record keeping requirement applies to each category of financial institution that has a requirement to file SARS: 31 CFR §§1024.320(c) [mutual funds]; 1025.320(d) [insurance companies]; 1026.320(d) [futures commission merchants and introducing brokers in commodities]; 1020.320(d) [banks]; 1023.320(d) [brokers or dealers in securities]; 1022.320(c) [money services businesses]; and, 1021.320(d) [casinos].
49. http://bsaefiling.fincen.treas.gov/main.html.
50. See "FinCEN to Implement SAR Acknowledgements and Validations for BSA E-Filing Submissions," (http://www.fincen.gov/whatsnew/html/20090826.html).
51. See http://www.fincen.gov/whatsnew/pdf/E-File_Brochure.pdf.

Characterizations of Suspicious Activity

Institutions frequently seek the guidance of FinCEN's Regulatory Helpline regarding characterizations of suspicious activity. There are several resources available that address these inquiries. In particular, banks should review the FFIEC BSA/AML Examination Manual, Suspicious Activity Reporting Overview, Identifying Underlying Crime. In addition, all financial institutions can find guidance published in October 2007 by FinCEN in The SAR Activity Review Issue 12, Section 4 under the topic of "Definitions and Criminal Statutes for the Suspicious Activity Report Characterizations of Suspicious Activity."

Section 3 — Law Enforcement Cases

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

Contributing editors: Shawn Braszo, Michael Hall, Jamie Hasken, Sean Evans, Liz Mathis, James Emery, Nivine Hanna, and Jack Cunniff.

This edition of *The SAR Activity Review* highlights the use of BSA data, particularly SARs, by providing specific examples of how the detection and analysis of suspicious transactions by financial institutions led to the prosecution of criminals in a wide range of cases. In the first case, financial institutions filed detailed summaries of structuring and debit transactions on a subject who was already of interest to law enforcement. In another case, an agent reviewing SARs filed in the local area discovered a series of structured transactions that, in turn, led to the arrest and prosecution of several individuals who eventually pleaded guilty to hiring illegal aliens. Even in cases not started by SARs, BSA records can greatly enhance an investigation. In one case, a bank noticed unusual transactions on the part of an auto dealer who was knowingly selling cars to drug traffickers and evading reporting requirements. This information helped solidify the government's case against the auto dealer. In all the cases, diligent financial institutions filed reports that proved crucial to convictions.

SARs Lead to Structuring and Tax Convictions

While investigating a subject of interest because of previous criminal activity, Federal agents found multiple SARs indicating repeated cash-out transactions designed to avoid reporting requirements. Investigators found SARs filed over several years on an owner and operator of a business, and his wife, detailing a pattern of structuring. One SAR noted that over 30 cash withdrawals were made in a 90-day period, all for just under $10,000.

In addition, another SAR noted that over a period of more than 6 months, there were nearly 250 debits totaling over $1,700,000, and of these debits there were more than 50 totaling over $1,500, which appeared unusual to the filer. Banks filed almost 200 Currency Transaction Reports (CTRs) on the defendants' business, indicating possible knowledge by the defendants of the reporting requirement. Moreover, the majority of the CTRs indicated cash-out activity which continued for several years.

Each of the defendants admitted that they moved large amounts of money, totaling millions of dollars, from the business' bank accounts into their personal bank accounts, ultimately withdrawing cash from the personal accounts in a series of withdrawals, each just under $10,000, over consecutive days. The defendants used the money for personal expenditures by (1) using cash to purchase money orders and bank checks that were then used for personal expenditures and (2) by paying third parties to purchase bank checks and money orders on behalf of the defendants.

The defendants designed the scheme in order to conceal the actual profits of the business and evade federal income tax. One defendant's banking activity was designed to further this evasion by avoiding the requirement that financial institutions file a CTR with FinCEN for any cash transactions exceeding $10,000. Similarly, the defendants conspired to avoid U.S. Postal Service reporting requirements for purchase of $3,000 or more in money orders from any one location in a single day by conducting a series of transactions over consecutive business days and in various locations. The defendants eventually pleaded guilty to structuring and tax charges.

SARs Aid Investigators in Case Where an Auto Dealer Laundered Drug Proceeds

SARs provided helpful information to investigators in making a case against an auto dealer and several associates involved in a drug trafficking and money laundering organization. During a 5 month investigation, federal agents uncovered a scheme that involved cash purchases at the dealership of cars by drug dealers. The cash purchases were in excess of $10,000, requiring reporting on FinCEN Form 8300, *Report of Cash Payments Over $10,000 Received in a Trade or Business*, however the auto dealer recorded selling the cars for under $10,000. Local financial institutions filed multiple SARs describing the suspicious and frequent deposits by the auto dealer, which aided in the investigation.

Two SARs were filed by a depository institution following an account review and the discovery of unexpected commingling of funds generated from two different businesses. The filer had identified checks made payable to the dealership that were deposited into the account of the defendant and another business. The bank described that business as a high-risk entity, and reported that the transactions were indicative of a business relationship that is not the type expected for a business account. SAR information gave investigators insight on the auto dealer's unusual bank deposit activity and helped identify two other accounts he was using.

According to investigators, the auto dealer met an individual who was a member of a drug-trafficking organization based in a Western state that was distributing illegal drugs from that state to buyers in the Midwest. The auto dealer eventually met other members of the drug ring, and, over time, engaged in multiple transactions with the traffickers in which he accepted cash for cars.

In one instance, the auto dealer sold a luxury automobile to the drug dealer for over $10,000 in cash. However, in an attempt to evade the requirement to file a Form 8300 with FinCEN, the auto dealer had the paperwork drawn up to reflect a purchase price of less than $9,000.

In another instance, the auto dealer was approached about buying a used car in cash from future marijuana sales. The dealer informed the buyer that he could evade law enforcement's notice by preparing paperwork saying the car sold for under $10,000, when the actual price would have exceeded that amount.

The dealer pleaded guilty to a charge of conspiracy to launder money derived from proceeds of illegal activity and was sentenced to almost 3 years in prison and ordered to forfeit more than $85,000. More than a dozen others connected to this case have been convicted of charges that include counts of conspiracy to distribute illegal drugs. Their sentences range from 30 months to more than 200 months imprisonment.

While the case was not initiated by SAR filings, a Federal agent said that the BSA database was one of the first places law enforcement researched after the dealer was identified as a target based on information provided by a co-conspirator. He estimated that his agency uses the database in over 95% of its cases.

FinCEN Data Proves to be Instrumental in Fraud Case

In a case propelled by information found in BSA records, an individual pleaded guilty to numerous charges, including the production of false identification documents. Notably, as soon as investigators became aware of the suspect's activity they queried BSA records and found details related to his criminal enterprise. Information reported on a SAR described illicit business activity and laid the groundwork for various seizures. Investigators repeatedly emphasized the importance of SARs to the case.

Federal investigators said that this case began when postal workers noticed an unusual amount of overnight mail sent to a post office box under the control of the defendant, but under a fictitious name. As the investigation progressed, agents queried BSA records and found several important SARs. One SAR revealed fictitious company names, bank account information, and a witness to the fraud. Investigators stated that through the use of records filed in compliance with the BSA, they were able to conclude that the defendant was running a cash-intensive business.

A SAR from a different bank noted that the defendant's business transactions showed nearly 40 currency deposits totaling over $170,000 within a 3-month period. The SAR also revealed debits from accounts showing expenditures for items such as entertainment, dining, jewelry, and electronic purchases. The bank did not find expected business expenses, such as payroll, office supplies, and tax payments.

According to investigators, the defendant produced and distributed false driver's licenses to underage teenagers throughout the United States through a referral e-mail account. The profits from the illegal business were structured into bank accounts and laundered by purchasing assets. The defendant operated this false driver's license operation by creating and mailing false driver's licenses and receiving documentation and cash through the U.S. mail using a post office box obtained in a fictitious name. The false licenses distributed by the defendant were high quality counterfeit state driver's licenses.

Federal agents executed a search warrant at the defendant's residence and among the items located and seized was cash in excess of $800,000 and illegal drugs and drug paraphernalia. After waiving his Miranda rights, the defendant admitted that all the drugs in the residence belonged to him. The defendant also stated that he had made at least $1 million from his false driver's license scheme. In his plea agreement, the defendant agreed to forfeit the cash found in his house, a new model luxury vehicle, real property, jewelry, numerous computers and software programs, and weapons and ammunition.

SAR Initiates Case that Leads to Guilty Pleas for Hiring Illegal Aliens

In a case initiated from SARs, Federal agents uncovered two businesses that were hiring illegal aliens in order to provide skilled and unskilled labor services to area warehouses. The businesses then paid the illegal aliens in cash, with funds withdrawn by the president and office manager in amounts under $10,000 to avoid CTR requirements and disguise the illicit payments to employees. The investigation began when a Federal agent researching SARs noticed the high total amount of the structured withdrawals.

One bank filed a SAR on the defendants for structuring activity over a 3-month period, detailing more than 30 cash withdrawals, each for just under $10,000, and totaling over $300,000. A different branch of the same bank filed multiple SARs on the defendants for over 100 structured cash withdrawals over a period of nearly a year, virtually all for less than $10,000. The total amount reported on the SARs was over $1,000,000. Another bank filed a SAR on the defendants for structuring more than two dozen cash withdrawals over a 6-month period, totaling over $300,000. All of the withdrawals were for amounts just under $10,000.

The defendants hired the illegal aliens to build the employee pool of their two businesses. They did not require employees to provide documentation of their immigrant status or their lawful right to hold employment in the United States. One company that hired workers from the defendants requested social security numbers for the undocumented aliens but the defendants provided only fraudulent numbers. In addition to paying the illegal aliens in cash, the defendants failed to deduct payroll tax and other such items from their pay.

A Federal agent investigating the case described the financial activity as a "blatant case of structuring." Both defendants pleaded guilty, with one receiving prison time and the other receiving house arrest and probation. A Federal judge also ordered the forfeiture of over $450,000 in proceeds obtained as a result of the criminal activity.

Proactive Review of SARs Leads to Long Prison Sentences for Drug Traffickers

Through a proactive review of SARs, a Federal agent identified records detailing structured transactions, unusual withdrawals, and unexplained wire transfers. The subsequent investigation uncovered over $2 million in cash and wire transfers from a drug-related money laundering conspiracy involving individuals in two states.

The case was initiated when a Federal agent uncovered SARs filed by depository institutions and by MSBs who reported over $2 million in cash transactions through different bank accounts in the respective states, as well as wire transfers originated at MSBs.

Two financial institutions filed SARs on the defendants detailing substantially large amounts of money structured into banks and then withdrawn. One SAR noted that in just over a year the defendants were responsible for more than 200 deposits totaling nearly $400,000, of which most was cash. The bank reported that the subjects appeared to be attempting to structure transactions, due to multiple deposits they made on the same day.

The agent reviewing BSA records found the SARs filed on the defendants and some of their associates. Many of the SAR narratives noted that the subjects made numerous, substantial deposits and withdrawals with no explanation for the source of the funds, such as normal business expenses. One SAR noted that a defendant was evasive when questioned about the business. In addition to moving money through various banks, the defendants used numerous individuals to structure money into MSBs at various locations across two states and then wire the money to locations in the United States and overseas. One SAR-MSB noted that the transactions went through more than 90 MSBs. From the MSBs, the funds were transferred to various "business" locations linked to the defendants. In total, financial institutions filed four SARs, three SAR-MSBs, and more than 10 CTRs on the defendants.

The investigation revealed that the two defendants were leaders of a prescription drug trafficking scheme that sent money from one state to another where other subjects used the funds to buy illegal prescription drugs. The defendants hired additional traffickers to transport the drugs, smuggling the illegal prescription drugs from one state to another state where they were distributed. After selling the drugs in their home state, the traffickers sent the money back to the originating

state, where it was used to purchase more drugs, luxury cars, and other property. Investigators also identified two doctors who wrote fraudulent prescriptions used by the drug dealers to obtain the illegal prescription drugs.

At one point, a state police officer, unaware of the Federal investigation, stopped one of the drug traffickers for a routine traffic violation. The police officer found drugs in the trafficker's car, which the trafficker admitted he had just purchased with cash. Other local police investigators later identified other drug dealers without jobs but who were driving luxury cars. When stopped for traffic violations, police found that the dealers often carried thousands of dollars in cash.

Federal agents started the investigation of this conspiracy based solely on the SARs. The investigation proceeded with the help of local police, including the use of surveillance techniques. A Federal agent reported that this investigation resulted in the complete dismantlement of the money laundering organization, the elimination of the source of supply, incarceration of the organization's leaders and members, and the seizure of the organization's assets. The trial marked the end of a one-year investigation into a drug trafficking and money laundering conspiracy operating in two states.

The defendants convicted at trial received more than 20 years in prison. Other drug traffickers and money launderers involved in this conspiracy pleaded guilty and received lower prison sentences. A Federal judge awarded the government more than $250,000 in seized assets, and imposed more than $3,600,000 in personal monetary judgments.

SAR Referral Leads to the Discovery of a $100 Million Mortgage Fraud and Foreclosure Rescue Scheme

Investigators uncovered a large-scale mortgage fraud scheme that originated from a SAR filed on a subject, who turned out to be a victim of the fraud scheme. In addition to filing the SAR, the filing institution also notified the district attorney's office, which opened the investigation and eventually uncovered the fraud.

A financial institution filed the SAR to report that tax lien had been forged. However upon investigation, the district attorney's office determined that the subject of the SAR was in fact a victim of fraud, in part by suspects who forged documents related to the tax liens. As the investigation continued, the district attorney's office uncovered the mortgage fraud that led to the indictments.

The 10-month investigation leading to the indictment uncovered a criminal enterprise that, through a network of co-conspirators and accomplices, located distressed residential real estate properties in order to perpetrate a racket to defraud lending banks through fictitious sales of those properties. The conspirators caused the banks to front millions of dollars to finance the purchase of these properties. The conspirators then retained most of the cash while leaving the banks with properties that were, in reality, worth considerably less than the value claimed in appraisals.

In one transaction, the defendants created an appraisal report for a duplex with a stated value of nearly $500,000. In actuality, the property was a vacant lot. One of the defendants in the case was paid to develop a false appraisal, after which the documentation was changed to indicate a certificate of occupancy for a two-family structure. This false documentation was then used to close the deal with the bank, which resulted in fraudulently obtained proceeds of nearly $500,000.

The larcenies in the indictment charged the defendants with stealing over $11 million in lending proceeds through trickery and fraud, mostly from banks. The combined efforts of the criminal enterprise appeared to have defrauded banks of almost $100 million. The lenders promptly securitized and sold the fraudulently obtained mortgages into the secondary market as collateralized debt obligations. Rating agencies assigned qualitative values to instruments backed by the securitized mortgages.

The local district attorney indicted approximately a dozen individuals and a mortgage origination company who were convicted later for perpetrating over $100 million in mortgage fraud over a 4-year period. According to investigators, this is a text book example of how the filing of one SAR, followed by immediate referral to law enforcement by the filer, led the district attorney's office to a different scheme involving one of the co-conspirators. The office followed up on the SAR and started investigating the conduct of the co-conspirator, which led to addition criminal violations. The conduct set forth in the indictment - the sham closing/ straw buyer scheme - was not the same scheme identified in the SAR. But without the filing of the initial SAR, investigators would not have learned of the scheme reflected in the indictment.

SARs Identify Huge Check-Kiting Scheme by Auto Dealer

SARs initiated the investigation of an automobile dealer who held several accounts at different institutions and continually transferred funds among the accounts, which caused the accounts to be overdrawn by millions of dollars. In addition to filing the SARs, the bank also notified law enforcement. The SAR narratives described the bank's relationship with the defendant and noted that he received a loan for his automobile dealership; however, the defendant did not make payments on the loan.

The defendant wrote checks on accounts that he controlled and deposited these checks into other accounts that he operated, all the while knowing there were insufficient funds in the accounts against which the checks were drawn. As a result of this check-kiting scheme, one of the auto business accounts was overdrawn by more than $6 million and another by almost $200,000.

As part of its business relationship with the auto dealership, the bank allowed the dealership to scan items for deposit into, and to initiate wire transfers out of, the account. The bank also made the proceeds of checks deposited into the auto dealership's account available for immediate withdrawal, without waiting for the checks to clear. The defendant took advantages of these privileges to facilitate the check-kiting scheme.

A Federal court sentenced the automobile dealer to several years in federal prison for his involvement in a multimillion-dollar bank fraud and money laundering scheme. The defendant was also convicted on charges resulting from a wire fraud scheme in which the defendant approached a former business customer for a loan in excess of $400,000 that he claimed would be used to purchase recreational vehicles for re-sale. He provided the former customer with a false personal financial statement that claimed that his net worth exceeded more than $6 million. Charges were also brought against him related to the false representation of his financial status when attempting to obtain a loan.

SARs and 314(b) Call Lead to Guilty Plea in Ponzi scheme

In a case initiated from a proactive review of SARs, an individual pled guilty to fraud when authorities discovered a scheme to defraud individuals and businesses out of millions of dollars. The SARs which triggered the investigation described in detail transactions related to the fraud. In addition, the 314(b) provision of the PATRIOT Act enabled institutions to work together and share information, resulting in the closing of suspect accounts and slowing the spread of the fraud.

The case began when a SAR review team identified reports filed by a financial institution with a total dollar amount of several million dollars. The defendant opened an account with a small cash balance and soon deposited more than $100,000. He then sent an out-going wire for over $100,000. Several days later, he attempted to deposit a check withdrawn from another bank for several million dollars and then wire the funds out of the bank. The bank put a 5-day hold on the check to verify that the funds existed. The defendant asked for the check back the next day. The bank later reported that the check had been altered and the true amount was for only a few hundred dollars. The bank also conducted Internet queries on the defendant and found links to lawsuits filed against him.

A SAR filed a few weeks later by another bank described fraudulent activity by the defendant. The bank reported that the defendant opened a new account and made deposits that totaled about $10,000. However, the bank soon found itself with checks totaling over $150,000 for which there were insufficient funds to cover the payments. The bank made a 314(b) call to the other financial institution where the defendant attempted to deposit the altered check and learned of the defendant's activities.

The second bank explained in the narrative that while their SAR filing reported activity on checks returned for insufficient funds, there were strong indications of fraud and deception that point to a possible Ponzi scheme. In addition to the SARs filed on the defendant, casinos filed more than 20 CTRs on the defendant over a 3 year period.

Prosecutors charged the defendant with wire fraud occurring over a period of more than 2 years. The essence of the scheme to defraud was the use of materially false and misleading statements and omissions of material fact in the solicitation of investment/loan funds from various family members, friends, and business acquaintances, purportedly for funding purchases for existing business contracts.

The funds, unbeknownst to the investors, were actually used, among other things, to pay off previous investors, other existing business debts and obligations, underwrite gaming activity, and purchase a personal residence and automobiles for cash.

Because of this scheme, victims suffered a combined loss of more than $3,500,000. The defendant admitted that he utilized the U.S. Postal Service to take money under false pretenses. He was charged with possession of counterfeit checks with the intent to deceive. The defendant pled guilty in federal court to mail fraud and has agreed to pay more than $3,500,000 in restitution.

Section 4 — Issues & Guidance

This section of *The SAR Activity Review* discusses current issues raised with regard to the preparation and filing of SARs and provides guidance to filers.

The U.S. Trustee Program's Civil Enforcement Activity Targets Bankruptcy-Related Mortgage Fraud and Mortgage Rescue Schemes

By Sandra Taliani Rasnak, Assistant Director for Criminal Enforcement, Executive Office for United States Trustees

The Financial Crimes Enforcement Network (FinCEN), in consultation with the United States Trustee Program, Federal Bureau of Investigation (FBI), and United States Department of Housing and Urban Development's Office of the Inspector General (HUD-OIG), contributed to this article highlighting the problem of bankruptcy-related mortgage fraud. As noted in FinCEN's 2010 Mortgage Fraud Report, the inter-relationship between bankruptcy and mortgage fraud is increasing.[52] *This article contributes to the continuing efforts within the President's Financial Fraud Enforcement Task Force to identify potential mortgage loan fraud and potential abuse of the bankruptcy system to facilitate mortgage fraud.*

Combating mortgage and mortgage rescue fraud and abuse is one of the top priorities of the United States Trustee Program ("USTP" or "Program")[53] and, over the last several years, the Program has dedicated significant civil and criminal enforcement resources to this effort. Internal detection by the USTP of bankruptcy

52. See http://www.fincen.gov/news_room/nr/html/20110328.html.

53. The United States Trustee Program is the component of the Department of Justice responsible for overseeing the administration of bankruptcy cases and private trustees under 28 U.S.C. § 586 and 11 U.S.C. § 101, *et seq*. To further the public interest in the just, speedy, and economical resolution of cases filed under the Bankruptcy Code, the Program acts to ensure compliance with applicable laws and procedures. It also identifies and helps investigate bankruptcy fraud and abuse in coordination with United States Attorneys, the Federal Bureau of Investigation, and other law enforcement agencies. For more information about the USTP, see http://www.justice.gov/ust/index.htm.

related mortgage and mortgage rescue schemes, as well as Program investigations of referrals from the bankruptcy court, private trustees, bankruptcy clerks, and other third parties, have enabled the Program to uncover potential wrongdoing and pursue appropriate civil enforcement actions against those who prey upon vulnerable consumers. When criminal conduct is suspected, the Program refers the alleged perpetrators and provides assistance to its law enforcement partners. These efforts are more fully discussed in several articles published in the *American Bankruptcy Institute Journal*.[54]

As part of its civil and criminal enforcement efforts, the Program also serves on several interagency working groups of national task forces such as the Financial Fraud Enforcement Task Force ("Task Force") established by President Obama in November 2009. Led by Attorney General Eric Holder, the Task Force brings together civil and criminal resources at all levels of government to hold perpetrators of financial fraud accountable. The Program's participation on national and local working groups further enhances its ability to detect and fight schemes that utilize a federal court system as a tool in victimizing those in financial distress.

This article describes several common bankruptcy-related mortgage fraud and mortgage rescue schemes, discusses the USTP's role in combating these schemes, and provides tips to financial institutions on detecting such unlawful activity.

Bankruptcy-Related Mortgage Fraud and Rescue Fraud Schemes

The FBI, a key USTP law enforcement partner, defines mortgage fraud as "a material misstatement, misrepresentation or omission relied upon by an underwriter or lender to fund, purchase or insure a loan." This definition focuses on conduct that harms lenders, such as providing false information on loan applications.

Consumers, however, also can be harmed by bankruptcy-related mortgage fraud. The perpetrators of mortgage foreclosure rescue fraud schemes use the federal bankruptcy court system as a means to defraud vulnerable consumers in jeopardy

54. Gail Geiger and Sandra Taliani Rasnak, "USTP Actions against Mortgage Fraud, Abuse Are Part of FFETF Sweep," *ABI Journal*, July-August, 2010, p.20; Sandra Taliani Rasnak, "USTP's Civil Enforcement Activity Targets Mortgage Fraud and Mortgage Rescue Schemes," *ABI Journal*, March, 2010, at 72-73 (portions of this article are incorporated herein and are reprinted with the permission of the *ABI Journal*); Sandra R. Klein "USTP Initiative Combats Bankruptcy-Related Mortgage and Real Estate Fraud," *ABI Journal*, July-August 2009, p. 18; Sandra R. Klein and Philip Crewson "USTP's Report on Criminal Referrals Highlights Criminal Enforcement Activity," *ABI Journal*, November 2009, p. 20.

of losing their homes to foreclosure or eviction. The filing of a bankruptcy case triggers the automatic stay, which immediately stops all collections actions. Often, the perpetrators of these schemes take advantage of the automatic stay, using it to give consumers the impression that the perpetrators' false promises of saving their homes are true since collection activities cease – at least temporarily. In some schemes, perpetrators use the bankruptcy system by recommending to consumers that they file bankruptcy to eliminate their unsecured debt and thereby position themselves to buy back their houses as part of a sale-lease back scheme. Furthermore, sometimes the perpetrators themselves file bankruptcy to discharge the debt they incurred as part of their mortgage fraud schemes.

The following highlights some examples of mortgage fraud schemes that use the bankruptcy system based upon recent prosecutions around the country. This information is intended to assist financial institutions in identifying illicit activities that intersect with their customers' transactions. This is not an exhaustive list of common fraud schemes. The associated "red flags" indicate only possible signs of fraudulent activity. No single red flag will definitively prove fraud, and one may apply to various types of fraud schemes. It is, therefore, important to view any red flag in the context of other indicators and the facts of the transaction. In some cases, the fraudulent activity may involve more than one type of fraud scheme or multiple actors.

Three types of bankruptcy-related mortgage fraud and rescue fraud schemes – financial consultant schemes, sale-lease back schemes, and reverse mortgage schemes – are explained below.

Financial Consultant Schemes

The financial consultant scheme is one of the most common mortgage rescue frauds encountered in bankruptcy. In this scenario, the perpetrators falsely tell desperate homeowners that, for a fee, they can help the homeowners save their homes by working with their lenders to stop foreclosure and modify or refinance their loans. Perpetrators identify homeowners through advertising on TV, on radio, in local newspapers, or on the Internet; through connections with churches and other affinity-based ethnic groups; or through foreclosure lists available from local governmental agencies. Homeowners are told to make their mortgage payments to the perpetrators or are required to pay the perpetrators a monthly consulting fee, or both. Of course, the perpetrators do not contact the lenders. Instead, they file serial fraudulent bankruptcy cases in the homeowners' names, sometimes without the homeowners' knowledge or consent, to use the automatic stay to stop the foreclosure.

In a variation of this scheme, homeowners are directed by the perpetrators to quitclaim fractional interests in their homes to fictitious individuals or businesses. Bankruptcy cases are then filed serially in the names of the fictitious individuals or businesses to continue the operation of the automatic stay. A third variation involves the perpetrators transferring fractional interests to unsuspecting individual debtors with pending bankruptcy cases without their knowledge or consent. Under any of these scenarios, because collection activity has been suspended, homeowners mistakenly believe that the perpetrators have fulfilled their false promises, and the homeowners' continue to pay the perpetrators.

Red Flags to Financial Institutions of Financial Consultant Schemes

- Mortgage payments stop being made. Mortgage payments abruptly stop with no contact from the homeowner and/or default occurs on the mortgage within a month or two after the loan is made.
- The foreclosure process is stayed by a bankruptcy filing. The filing of the bankruptcy case may be in tandem with the sudden failure to make regular mortgage payments.
- The debtor in the bankruptcy case that stayed the foreclosure is not the borrower.
- The debtor does not disclose a fractional interest and/or other ownership in real property in his/her bankruptcy documents. Failure to disclose such interests may indicate a fractional interest or property transfer scheme.
- Serial bankruptcy cases are filed and/or numerous lenders file motions seeking relief from the automatic stay to proceed with foreclosure and/or eviction actions. Where the perpetrators file serial bankruptcy cases, especially those involving fractional interest schemes, financial institutions should expect to see other lenders filing motions seeking relief from the bankruptcy automatic stay as well.

Sale-Lease Back and Property Transfer Schemes

In the sale-lease back scheme, the perpetrator gains control of an individual's home and skims real or manufactured equity from the property. The perpetrator tells the homeowner that the home can be saved by selling it to a third-party purchaser chosen by the perpetrator – also known as a "straw purchaser" – and then renting it back from the purchaser for an amount less than the homeowner's current

mortgage payment. Frequently the perpetrator promises that the homeowner can buy the home back within a certain period of time at the same price at which it was sold, thus protecting the homeowner's "equity." In some schemes, the perpetrator persuades the homeowner to file bankruptcy in order to repair the homeowner's credit and place the homeowner in a better position to obtain financing to buy back the home.

The perpetrators of these schemes profit by gaining control of the properties and obtaining fraudulent loans in the straw purchasers' names based on inflated appraisals of the properties' value. The inflated sales price creates a significant amount of "fake" equity that the perpetrators take through fees that are included in the closing payoffs. Moreover, the perpetrators may arrange to have any remaining sales proceeds signed over to them, rather than to the homeowners. The straw purchasers usually receive some money at closing for each property purchased. Eventually the straw purchasers file bankruptcy to discharge the mortgage debt incurred in their names. Usually, they do not disclose payments received at closing in their bankruptcy documents. In the end, the homeowners lose their homes.

In a related scheme, homeowners desperate to sell their homes are persuaded to "sell" their property to the perpetrators based on false promises that the perpetrators will obtain new loans to pay off the homeowners' existing mortgages. The perpetrators do not get financing, but instead put renters in the properties and collect the rents. No mortgage payments are made and the financial institutions are not notified of the title transfer. To further the scheme, the perpetrators may file incomplete serial bankruptcy cases in the homeowners' and/or renters' names without their knowledge or consent for purposes of obtaining the automatic stay to stop the collection actions.

Red Flags to Financial Institutions of Sale-Lease Back Schemes

- The bankruptcy documents are incomplete. The lack of complete documentation may indicate a potential for fraudulent activity. In some cases, the bankruptcy filings are not in the name of the borrower.
- The debtor does not disclose that property was transferred just before the bankruptcy filing and/or does not disclose owning any property. Despite this failure to disclose the property transfer or ownership, the debtor's residential address is listed as the address of the property subject to the mortgage.

- The debtor claims that the bankruptcy case was not authorized and/or was not aware that a bankruptcy was filed on his or her behalf. This may indicate that a fraudulent filing was made in the debtor's name by another party.
- The bankruptcy case is not pursued by the debtor and is short-lived. As a result, financial institutions may find it difficult to gather detailed information beyond the filing information about the debtor or the suspected perpetrators.
- The debtor's bankruptcy documents show the purchase of multiple properties over a relatively short period of time without the income or assets to support such purchases. This may indicate that the debtor was a straw purchaser in a mortgage or mortgage fraud rescue scheme.

Reverse Mortgage Schemes

A scheme that is becoming more widespread involves federally-insured home equity conversion mortgages ("HECMs")[55], which are sometimes referred to as reverse mortgages. In coordination with HUD-OIG,[56] FinCEN published an advisory calling attention to this type of mortgage fraud activity.[57] In that advisory, FinCEN detailed a number of specific schemes and red flags to assist financial institutions in identifying this fraudulent activity.

Perpetrators of bankruptcy-related HECM schemes may be organized rescue fraud rings, neighbors, or members of the homeowner's family. In many cases, the borrowers are in poor health and may suffer from memory loss. These vulnerable homeowners are persuaded to sign paperwork prepared by the perpetrator, including power of attorney authorizations. Once the perpetrator obtains the necessary signatures, the perpetrator takes control of the borrowing process and elects to receive the home equity loan proceeds in a lump sum. If the homeowner does not have equity in the home, the perpetrator typically generates a false appraisal to manufacture equity. The perpetrator pockets the loan proceeds, and the homeowner loses the equity and may be unable to retain the home. In some situations, the perpetrator may also file bankruptcy on behalf of the homeowner to extinguish unsecured debt the perpetrator may have incurred in the homeowner's name or to stop other related collection activities.

55. HECM loans are available to individuals who are 62 years of age or older.
56. Department of Housing and Urban Development, Office of Inspector General.
57. See: "Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Home Equity Conversion Mortgage Fraud Schemes," FIN-2010-A005 at http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-a005.pdf.

Suspicious Activity Reporting

The activities of financial institutions may intersect with a mortgage fraud scheme involving the use of bankruptcy proceedings in several ways. For example, the financial institution may be the current holder of the underlying mortgage loan and may become aware of such scams through its interactions with customers or upon notice of a bankruptcy filing. In addition, those perpetrating mortgage fraud schemes involving the use of bankruptcy may seek the services of financial institutions for the purpose of receiving, depositing, or moving illicit funds relating to the scams.

Consistent with the standard for reporting suspicious activity as provided in 31 C.F.R. Chapter X, if a financial institution knows, suspects, or has reason to suspect that a transaction involves funds derived from illegal activity or that activities conducted or attempted by, at, or through the financial institution indicate money laundering, terrorist financing, or other violation of law or regulation, the financial institution should file a SAR.[58] As noted in FinCEN's *SAR Narrative Guidance Package*,[59] financial institutions must provide complete and sufficient descriptions of known or suspected criminal violations or suspicious activity in the SAR narrative sections.

To assist law enforcement in its efforts to target mortgage-related fraudulent activity involving the use of bankruptcy proceedings, it is beneficial if financial institutions that detect such activity include the specific term "bankruptcy" within the narrative portions of all relevant SAR filings (in addition to other applicable recommended terms provided by FinCEN in previous mortgage fraud-related advisories)[60] and highlight the exact dollar amount(s) associated with the identified mortgage fraud. It is also beneficial to include all information available for each party suspected of engaging in this fraudulent activity in the Suspect/Subject Information section in the SAR filing. This includes an individual or company's name, address, email address, phone number, and any other identifying information.[61]

---

58. Financial institutions shall file with FinCEN to the extent and in the manner required a report of any suspicious transaction relevant to a possible violation of law or regulation. A financial institution also may file with FinCEN a SAR with respect to any suspicious transaction that it believes is relevant to the possible violation of any law or regulation, but whose reporting is not required by FinCEN regulations. *See*, e.g., 31 C.F.R. § 1020.320(a).
59. See http://www.fincen.gov/statutes_regs/guidance/pdf/narrativeguidance_webintro.pdf.
60. See http://www.fincen.gov/news_room/advisory/AdvisoryKeyTerms.html.
61. If multiple subjects are involved, the filer should include information within the report for each subject.

Conclusion

The United States Trustee Program, in coordination with its law enforcement partners, the Financial Fraud Enforcement Task Force, and FinCEN, is committed to combating mortgage and mortgage rescue fraud and abuse. The filing of SARs by financial institutions provides law enforcement with information that assists in identifying and addressing mortgage fraud schemes. Lenders and consumers alike benefit from the detection and pursuit of these unlawful schemes.

Organized Retail Crime – A Multi-Billion Dollar Problem

By Immigration and Customs Enforcement

Organized retail crime (ORC) refers to groups, gangs and sometimes individuals who are engaged in illegally obtaining retail merchandise through both theft and fraud in substantial quantities as part of a criminal enterprise. It is a growing problem throughout the United States that is affecting every consumer. ORC involves individuals known as "boosters", who are often members of organized criminal networks who convert the product for profit. To combat these networks, U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) is teaming with the retail industry and law enforcement at all levels. ICE HSI's focus is to combat these organizations by turning to federal anti-money laundering statutes that can carry severe penalties.

In July, 2009, ICE HSI initiated an ORC pilot program to help combat the transnational organized crime networks involved in this illicit activity. This pilot program was originally initiated in the Special Agent in Charge (SAC) offices located in Houston, Los Angeles, Miami, and New York. These four cities were selected due to the ties many ORC groups have to these areas. Since then, ICE HSI has become increasingly involved in investigations targeting organized retail crime due to the interstate and international shipments of stolen goods and the corresponding movement of illicit proceeds from the sale of these stolen goods. The interstate and international shipment of stolen goods is one of the specified unlawful activities which make charges related to Title 18 United States Code § 1956 – laundering of monetary instruments – possible.

Due to the overwhelming success of the ORC pilot program, ICE HSI launched the SEARCH initiative (Seizing Earnings and Assets from Retail Crime Heists) as an ongoing, national initiative. The SEARCH initiative is the first step in linking together federal, state and local law enforcement, prosecutors, and the financial and retail community to provide a multi-faceted approach to prosecuting and deterring individuals/organizations involved in ORC. The retail industry has provided significant support to this national initiative because, all too often, this type of organized, criminal activity is looked at as a local problem. Lack of visibility outside a jurisdiction can contribute to the appearance that it is a local problem. Federal investigations conducted by ICE HSI, and other law enforcement agencies, have proven the level and sophistication of criminal enterprises involved in ORC is often times much greater.

Additionally, profits generated from ORC represent a clear threat to the U.S. financial sector, as these profits are being laundered through U.S. and international financial systems. ORC rings look for and take advantage of vulnerabilities within these financial infrastructures to move and store their illicit proceeds. These organizations are very sophisticated, compartmentalized, and operate similar to criminal organizations involved in drug trafficking or human smuggling.

The SEARCH initiative will result in the execution of multi-faceted, multi-disciplined investigations which will subject ORC rings to simultaneous enforcement actions against multiple operational cells within their organizational structure. The primary goal of conducting comprehensive investigations, which simultaneously target the methods ORC rings earn, move, and store funds, is to generate the maximum amount of disruption and organizational chaos.

As part of the SEARCH initiative, ICE HSI will proactively work to identify and disseminate "red flag indicators" of suspicious financial transactions to assist financial institutions in developing the typologies necessary to proactively target and report on ORC rings attempting to launder their illicit proceeds from the sale of stolen goods. Based on past successful ICE HSI investigations into ORC, some indicators of suspicious banking activity have already been identified. Some of these indicators include the following:

- Business checks written to individuals versus legitimate suppliers and cashed at the banks where the checks originated from versus being deposited into another businesses bank account.
- Business checks written to cash on a regular basis in amounts that far exceed a business' petty cash requirement.

- Multiple checks on the same day consistently written in amounts less than $10,000, possibly to avoid reporting requirements, despite the fact that checks would not normally generate Currency Transaction Reports.
- Multiple checks written on the same day to cash to ensure the amount of each check written does not exceed $10,000.00.
- Multiple money orders in increments of $500 or less deposited into bank accounts where the remitter of the money order is the same as the authorized signers on the bank accounts for which the checks are being deposited.
- Cash deposits related to the questionable financial activities involved currency in $100 denominations.
- Fraudulent use of debit/gift cards, which are also referred to as stored value cards.
- Cashier's checks obtained from U.S. banks and tendered at foreign banks.
- Large bank wire transfers in exchange for product shipped via interstate commerce.

Since the inception of the ORC Pilot Program, ICE HSI has built strong partnerships with the retail industry as well as the National Retail Federation (NRF), and Retail Industry Leaders Association (RILA). Through these partnerships, and with the assistance of state and local agencies, ICE HSI has initiated more than 120 criminal investigations, affected 63 arrests, and seized over $6.4 million dollars in property as of July 31, 2011.

One example of a successful ORC investigation is Operation Milk Money. Operation Milk Money was initiated based on information that a large scale organization was involved in the theft and interstate transportation of stolen baby formula. The investigation identified the primary targets as Honduran nationals who were responsible for stealing and re-selling thousands of canned powder baby formula on a monthly basis with an estimated annual loss to the retail industry in excess of $1 million dollars.

ICE HSI Resident Agent in Charge (RAC) Winston-Salem, SAC Newark, the High Point Police Department and U.S. Department of Agriculture – Office of Inspector General (USDA – OIG) all participated in Operation Milk Money. This ICE HSI-led investigation targeted a large scale organization involved in the theft and interstate transportation of stolen baby formula. The primary subjects engaged in financial

transactions to conceal the nature, source, ownership, and control of the illicit proceeds earned from the sale of the stolen baby formula. Investigators discovered one target of the investigation structured approximately $208,744 in cash by making deposits in amounts less than $10,000 in an attempt to avoid FinCEN's reporting requirements. Multiple search and arrest warrants were executed in January 2011, resulting in 21 arrests (9 criminal and 12 administrative) and the seizure of approximately $160,000, seven vehicles, and a quantity of stolen baby formula valued in excess of $10,000.

Health Care Fraud

By FinCEN's Analysis and Liaison Division and Office of Outreach Resources

Health care fraud in the United States has become an increasing focus and area of concern for federal law enforcement who implemented a national strategy to combat the issue in May 2009. In this article, FinCEN presents some potential indicators of health care fraud, based on an analysis of related SAR filings, to assist filers in identifying and reporting suspicious activity that may indicate the existence of health care fraud.

Potential Indicators of Health Care Fraud

The following list of red flags identifies only possible signs of illicit activity. While many of these flags may be indicative of fraud in general, these activities have also been identified as activity directly related to fraud occurring in the health care industry.

Financial institutions should evaluate indicators of potential fraud in combination with other red flags and expected transaction activity. Additional investigation and analysis may be necessary to determine if the activity is suspicious.

Customer Identification and Expected Activity

- A personal account is receiving large dollar electronic funds transfers (EFTs) into the account and has large, even dollar payments going out of the account.
- A business account is established using an address that is shared by other companies, sometimes with the same owner or account signer listed.
- Multiple companies with similar names are located at the same address and share the same owner or account signer.

- A company switches from a business model not related to the health care industry to one which is related.
- The owner of a business is not the account signer. The account signer(s) for the business is not listed on any paperwork for the company.
- The account is located in a state other than where the doctor/company providing the service or receiving payment is located.
- Transfers are conducted from several apparently unrelated companies to the same one or two companies, which are in turn sending funds back to another account, and there is reason to believe that there may be common owners among the companies.
- A company is billing the Medicare program for multiple products/services (which are, in practice, provided by separate contractors under the Medicare program.)

Account and Transactional Activity

- An individual or a company maintains multiple bank accounts with the same financial institution and conducts transfers between the accounts that do not have an apparent reason or business purpose.
- A business account has no transactions for expected business related expenses (i.e., payroll, vendor payments, or utility expenses.)
- An account has a change in ownership followed by a significant increase in account activity.
- A business customer suddenly changes its mailing address to a P.O. Box, residential address or other non-descript address (which could be a sign of an account takeover.)
- A fraudulent company is created and named similarly to a legitimate company with the intent of using fraudulent checks meant to pass as checks drawn by the legitimate company.
- Checks drawn on a health care related business account, which in turn are being cashed at a check cashing service.
- Use of cashier's checks in lieu of checks or EFT to pay for goods, or make other payments from the account.

- Purchases of money orders in even dollar amounts which are made payable to a third party that does not appear to be business related.
- A business account has expenses that appear personal in nature (for vacations, purchase of goods or services).
- Hard-copy checks are received into an account as Medicare payments, when the standard form of payment is EFT.
- Checks made payable to the "IRS" which are intended to look like payments to the Internal Revenue Service (e.g., a fraudulent company that is using the initials "IRS" in its name.)
- A business account established with a small bank which in turn has funds moved to an account at a larger bank.
- An account opened with a minimum deposit that had no activity or minimal activity over an extended period of time suddenly begins to receive large or frequent deposits from a Medicare contractor.
- EFT deposits from Medicare immediately followed by a withdrawal for exactly the same amount by either check, wire transfer, cash withdrawal or ATM withdrawal within a day of the deposit.
- Checks from Medicare and/or HMO plans are endorsed over to a third party and either deposited into an account with no affiliation to the health care industry or cashed at a check cashing business.
- Checks from Medicare, Medicaid or an HMO deposited into accounts with no affiliation to the health care industry (such as a liquor store.)
- Financial transactions (wires, checks, etc.) with companies not involved in health care (automobile dealers, liquor stores, restaurants, etc.)
- The only checks written against the account are to the account signer or other companies affiliated with the account signer.
- Companies that allegedly provide durable medical equipment but show no expense transactions related to the purchase of those goods AND are billing Medicare or an HMO for supplying the goods.
- Significant withdrawals made from an ATM.

Insider Activities

- Employees of a financial institution overriding a hold that has been placed on an account identified as suspicious so that transactions can occur in the account.
- Employees assisting fraudsters in identifying dormant health care industry related accounts. Fraudsters gain access to account names and numbers and produce fake documents that allow them to close the accounts and withdraw any funds left in the account.

Suspicious Activity Reporting

In order to assist FinCEN and law enforcement in the effort to target instances of health care fraud, it is beneficial if financial institutions that detect potential suspicious activity related to such fraud include the term "health care fraud" in the narrative portion of all relevant SAR filings, in addition to selecting the appropriate characterization of suspicious activity in the Suspicious Activity Information section of the SAR form. The narrative should include an explanation of why the institution knows, suspects, or has reason to suspect that the activity is suspicious. It is also beneficial to law enforcement if, when filing a SAR related to health care fraud, a filer 1) identifies the company or insurance program that is providing incoming EFT's or checks associated with the suspicious activity and, 2) documents the names of companies, entities or individuals that are receiving frequent or large checks or EFT's from the subject account.

SAR Confidentiality and Disclosure

By FinCEN's Office of Compliance and Office of Outreach Resources

Historically, banking agency rules have stated that a SAR, and its predecessor, the Criminal Referral Form, were confidential. 31 U.S.C. 5318(g) granted authority to the Secretary of the Treasury to require financial institutions report suspicious activity, and further stated that anyone acting on behalf of the financial institution, be they a director, officer, employee, or otherwise, as well as employees of the Federal Government or of any jurisdiction within the United States, with knowledge of a SAR may not disclose to any person involved in the transaction that a SAR has been filed, other than as necessary to fulfill their official duties. The USA PATRIOT Act expanded SAR requirements to financial institutions that had not previously been required to report suspicious activity, such as broker/dealers and insurance companies.

The expectation of financial institutions that the confidentiality of SARs filed will be appropriately maintained is the basis for the extraordinary level of information sharing between the filing institutions and those who access and use the data. That expectation is also indicative of the level of public trust that institutions have placed in those who access the data.

FinCEN's regulations, while not specifically stating that SARs were confidential, nonetheless prohibited the notification of any person involved in a reported suspicious transaction that a SAR had been filed. That was often misinterpreted to mean that disclosure was prohibited only to the subject of the SAR. However, FinCEN had always interpreted the language much more broadly.

In November, 2010 FinCEN issued a final rule on the *Confidentiality of Suspicious Activity Reports*.[62] This rule served to clarify how, when, and to whom SAR information, and the existence of a SAR, may be disclosed. This article highlights two critical areas: the confidentiality of SARs and SAR information in general, and disclosure of SARs and SAR information in "fulfilling official duties consistent with the Bank Secrecy Act."

To clarify certain aspects of the SAR regulations, FinCEN amended the language regarding confidentiality to specifically state, "A SAR, and any information that would reveal the existence of a SAR, are confidential…" This wording was chosen to make it clear that the existence, or even the non-existence, of a SAR must be kept confidential, as well as the information contained in the SAR to the extent that the information would reveal the existence of a SAR. FinCEN also aimed to clarify any misinterpretation that the SAR must only be kept confidential from the subject of the SAR.

FinCEN specifically noted that even individuals and agencies acting in an official government capacity are subject to SAR confidentiality rules. Any officer or employee of the government may not disclose a SAR or information that would reveal the existence of the SAR, except as is necessary to fulfill official duties consistent with the BSA. Official duties include criminal, tax and regulatory investigations and proceedings. Therefore, for example, disclosure would be permitted to certain parties with regard to an investigation on money laundering or terrorist financing. However, a SAR disclosure is not permitted for matters of civil litigation, such as a divorce or a private debt collection. In addition, the rule explicitly states that disclosure to the media is not permitted.

62. See http://www.fincen.gov/news_room/nr/pdf/20101122.pdf.

Many valid reasons exist for law enforcement and regulators to have direct access to the FinCEN database, which includes SARs. However, not everyone within those agencies has access. Specific persons are given access to the database and permission is granted only after an appropriate background investigation is completed and training is conducted, which includes training on use of the database and maintaining the confidentiality of or information derived from a SAR.

Inappropriate disclosures of SARs can have various ramifications. A disclosure could compromise a criminal investigation and render useless countless law enforcement resources. A disclosure could also put the filer or filing institution in harm's way. For instance, a media article disclosing that law enforcement was able to indict individuals on terrorist financing charges because of a SAR filed by a certain financial institution could subject that institution to retaliation by the suspects or members of a suspected or known terrorist cell. If the person responsible for filing a SAR becomes known to the subject, that person might receive threats against their well being, or worse actually attacked with intent to injure or kill.

In instances where SAR confidentiality has been compromised, FinCEN investigates each allegation of improper disclosure and may take action against those responsible based on factors such as the gravity of the violation. These actions may include issuing a warning to the person or entity involved in the disclosure and civil penalties. In instances where the disclosure is criminal in nature, FinCEN may refer the matter to law enforcement. In some cases, FinCEN has restricted access to SAR information as a result of improper disclosure.

FinCEN also issued a guidance piece[63] on SAR confidentiality when the final rule was published which aimed to facilitate enterprise-wide risk management by allowing SAR sharing amongst U.S. affiliates within the corporate structure, under certain conditions. This guidance is a companion piece to the guidance that was issued in 2006 allowing the upward sharing of SARs to a parent company, subject to certain restrictions. Concurrent with the final regulation, FinCEN published an Advisory that highlighted for financial institutions and government employees – whether law enforcement or regulators – their responsibilities concerning confidentiality of SARs.

---

63. See *Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates* at http://www.fincen.gov/statutes_regs/guidance/html/fin-2010-g006.html and *Sharing Suspicious Activity Reports by Securities Broker-Dealers, Mutual Funds, Futures Commission Merchants, and Introducing Brokers in Commodities with Certain U.S. Affiliates* at http://www.fincen.gov/statutes_regs/guidance/html/fin-2010-g005.html.

It is critically important that financial institutions are confident that the information they provide to help in the fight against money laundering, financing of terrorism and other financial crime is appropriately protected by those to whom that information is entrusted. By strengthening and clarifying SAR confidentiality, FinCEN hopes to increase trust and security across our AML landscape.

Update: Elder Financial Exploitation

By FinCEN's Office of Outreach Resources

On February 22, 2011, FinCEN issued FIN-2011-A003, *Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation*.[64] The Advisory provided red flags for identifying suspicious activity and requested that financial institutions use the term "elder financial exploitation" when filing SARs with respect to such activity.

FinCEN issued the Advisory in conjunction with the publication, *Financial Institutions Outreach Initiative, Report on Outreach to Depository Institutions with Assets under $5 Billion*.[65] During the course of the outreach initiative summarized in that report, financial institutions repeatedly highlighted their efforts to combat elder financial exploitation. FinCEN's decision to issue the Advisory was a direct result of financial institutions' interest in and commitment to the issue.

The purpose of the Advisory was not only to help institutions detect suspected elder financial exploitation and report it using a standardized term; it was also to highlight how an institution's ongoing efforts to fight elder financial exploitation can complement its AML program.

Financial institutions have responded with a substantial increase in SARs reporting elder financial exploitation. This article provides preliminary feedback on filing trends and addresses common questions received by FinCEN's Regulatory Helpline.

Filing Trends

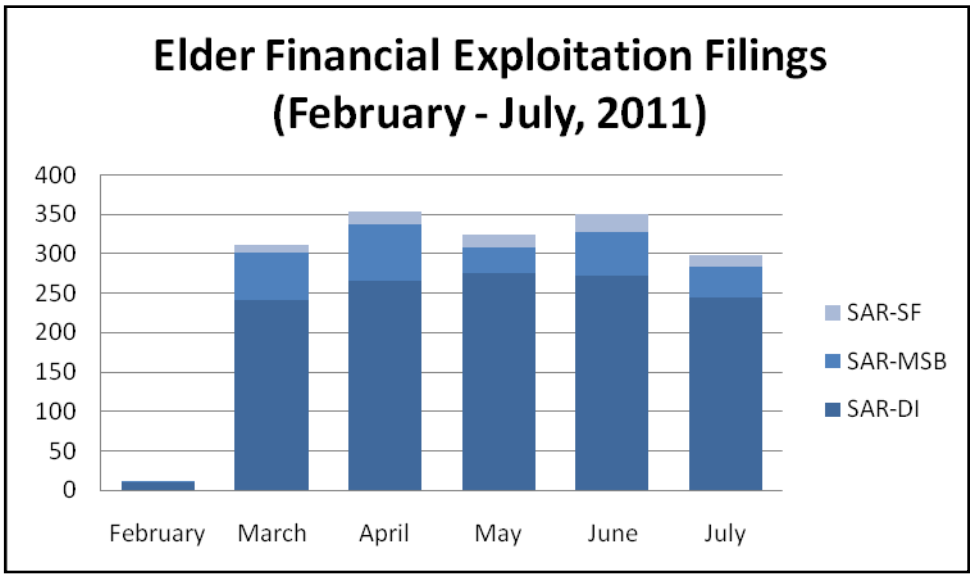
Between February 1 and July 31, 2011, financial institutions filed 1,649 SARs whose narratives contain the requested term, "elder financial exploitation." For ease of reference, we will refer to such reports throughout as "elder financial exploitation

64. See, http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2011-a003.pdf

65. See, http://www.fincen.gov/news_room/rp/reports/pdf/Banks_Under_$5B_Report.pdf

SARs." Graph 1 below displays the filing volumes in the months following the Advisory's release. The sections that follow provide additional information for each class of reporting entity.[66]

Chart 1



Depository Institutions

A total of 291 depository institutions[67] filed 1,308 elder financial exploitation reports during the selected time period. Three of these institutions filed from 150 to over 300 reports, while more than 250 institutions filed between one and three reports. Filers at branches located in 48 states, the District of Columbia, and Puerto Rico; the top states for branch locations were California (216 reports), Florida (48), Texas (38), New York (33), Washington (33), and Hawaii (33).

Filers co-reported a wide range of suspicious activity characterizations when reporting elder financial exploitation; 241 SARs reported credit card fraud.[68] The next most common characterizations were check fraud (195 filings) and identity

66. Sections cover depository institution SARs, the SAR-MSB, and the SAR-SF. No casinos filed elder financial exploitation SARs.
67. As identified by Filer EIN/SSN.
68. A single institution filed 220 of the 241 credit card fraud SARs.

theft (192 filings.)[69] Other commonly reported activities were Bank Secrecy Act/ structuring/money laundering (121), check kiting (83), mortgage loan fraud (46),[70] debit card fraud (38), counterfeit debit/credit card (37), and wire transfer fraud (35).

"Other" was the sole activity characterization selected in 548 of the depository institution elder financial exploitation SARs. For 434 of these, the corresponding description contained solely a variation on the term "elder financial exploitation" or "elder abuse." However, of the remaining 114, 43 referenced automated clearing house (ACH) fraud. Many also noted scams and other frauds.

Money Services Businesses

MSBs filed 259 elder financial exploitation SARs during the selected time period, all of which detailed wire transfer activity.[71] These were filed by nine institutions, which include both MSB principals and agents. The reports describe numerous situations in which customers sent wire transfers to domestic and foreign-located individuals who were unknown to them. Upon discussion with customers, filers uncovered apparent advance fee schemes,[72] online dating scams,[73] and scams in which individuals posed as friends or family members in need of emergency funds.[74] One report described a customer's attempt to send wire transfers after unknown individuals told her simply that she had to do so.

Another SAR reported that a customer sent over $75,000 to the same individual in a series of more than one hundred wire transfer transactions. Filers of several reports believed that senders had been instructed by the scammers to structure transactions.

---

69. Of the 192 identity theft SARs, credit card fraud was co-reported in 128. The co-reporting of credit card fraud with identity theft is noted in FinCEN's 2010 Strategic Analytical Report, *Identity Theft: Trends, Patterns, and Typologies Reported in Suspicious Activity Reports*

70. Eleven of these reports also used the acronym "HECM", the narrative term requested in FIN-2010-A005, *Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Home Equity Conversion Mortgage Fraud Schemes*, which FinCEN issued on April 27, 2010. See http://fincen.gov/statutes_regs/guidance/pdf/fin-2010-a005.pdf.

71. As reported on Item 19 of the SAR-MSB.

72. Advance fee schemes described included lottery and prize schemes. For further information on advance fee schemes, see *The SAR Activity Review – Trends, Tips & Issues*, Issue 4, http://www.fincen.gov/news_room/rp/files/sar_tti_04.pdf#page=55.

73. Such schemes are sometimes referred to as "sweetheart scams." For more information, see *Online Dating Scams, When Love Goes Wrong* http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt190.pdf.

74. Such schemes are sometimes referred to as "grandparent scams." For more information, see *Money Transfer Sams – The Grandparent Scam*, http://www.ftc.gov/multimedia/video/scam-watch/money-transfer/wire_vladeck-q2a.shtm.

In some instances, alert front line personnel at agent locations were able to intervene either directly with the customer or with the principal to stop a transaction from being completed. In certain situations, MSB principals reported adding both victim customers and SAR subjects to internal lists of individuals to whom they would deny wire transfer services.

Securities and Futures Industries

Institutions filed 82 elder financial exploitation SAR-SFs during the selected time period. The twenty-eight entities filing these reports included securities dealers, clearing and introducing securities brokers, investment companies, and insurance companies, among others.[75] Common suspicious activity characterizations indicated on these reports included embezzlement (32 reports), wire fraud (12), forgery (11), identity theft (11), and check fraud (10). "Other" was the sole activity characterization selected in over a third of the elder financial exploitation SAR-SFs.

The reports described both suspected embezzlement by family members as well as advance fee and investment scams for the benefit of individuals who were unknown to the elder customer. Two-thirds of the elder financial exploitation SAR-SFs reported that the activity involved the use of cash or cash equivalents, as compared with about 40% of all SAR-SFs filed during the same time period.[76]

Guidance

FinCEN's Regulatory Helpline frequently receives inquiries from institutions seeking guidance on filing elder financial exploitation SARs and reporting activity to law enforcement. One common question is where to provide the information of an elder victim who is not the subject of the SAR. Financial institutions may provide this information in the narrative.[77]

Another frequently asked question is what the dollar threshold is for reporting elder financial exploitation. The Advisory did not change any reporting requirements under the Bank Secrecy Act.[78] For example, for suspicious activity that does not involve insider abuse or computer intrusion, the dollar threshold at which it is mandatory for a depository institution to file a SAR is $5,000 where there is a known

75. As indicated in SAR-SF Item 51.
76. As reported on Item 23 of the SAR-SF.
77. See the Advisory, http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2011-a003.pdf
78. Financial institutions and employees may have separate requirements for reporting elder exploitation under state law.

suspect; where there is not a known suspect, the threshold is $25,000. A financial institution may also choose to voluntarily file a SAR in situations where dollar activity thresholds are not met.[79]

Institutions also ask about sharing SARs with appropriate law enforcement.[80] Consistent with, e.g., 31 CFR 1020.320(e), provided that no person involved in any reported suspicious transaction is notified that the transaction has been reported, institutions may disclose a SAR, or any information that would reveal the existence of a SAR, to FinCEN or any Federal, State, or local law enforcement agency. Under 31 U.S.C. 5318(g)(3),[81] such disclosures are provided safe harbor protection from civil liability, including with respect to both mandatory and voluntary SARs. However, we would refer financial institutions to the SAR disclosure rules, with specific reference to *FIN-2010-A014, Maintaining the Confidentiality of Suspicious Activity Reports*[82] for additional information as well as the article, *SAR Confidentiality and Disclosure*, published in this issue of *The SAR Activity Review*. If your institution has questions about sharing information with appropriate law enforcement, please contact FinCEN's Regulatory Helpline at (800) 949-2732.

Electronically Filing the Registration of Money Services Business (RMSB)

By FinCEN's Office of Outreach Resources

On July 18, 2011, FinCEN announced that any MSBs can now file its Registration of Money Services Business (RMSB) using FinCEN's Bank Secrecy Act (BSA) E-Filing System.[83]

---

79. Financial institutions shall file with FinCEN to the extent and in the manner required a report of any suspicious transaction relevant to a possible violation of law or regulation. A financial institution may also file with FinCEN a SAR with respect to any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by FinCEN regulations. See, e.g., 31 CFR § 1020.320(a).
80. See *The SAR Activity Review – Trends, Tips & Issues*, Issue 9, http://www.fincen.gov/news_room/rp/files/sar_tti_09.pdf#page=49, for more information about sharing SARs with law enforcement.
81. See, also, 31 CFR 1020.320(f)
82. See, http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2010-A014.pdf.
83. See "FinCEN Announces Electronic Filing for MSB Registrations," (http://www.fincen.gov/news_room/nr/html/20110716.html).

E-Filing is a free, web-based electronic filing system that allows an MSB to submit its RMSB through a secure network. An MSB will find E-Filing to be a faster and more convenient, secure, and cost-effective method of submitting its registration. In particular, the MSB will receive an electronic acknowledgement of its registration's acceptance within two business days of filing. An MSB also may use E-Filing to submit SARs and CTRs. In light of the new capability to file the RMSB electronically, FinCEN is addressing how E-Filing relates to the registration questions that MSBs and banks with MSB customers often raise with FinCEN's Regulatory Helpline.[84]

Filing deadlines

Use of E-Filing does not change existing registration filing deadlines.[85] An MSB can use E-Filing for an initial registration, as well as a renewal, re-registration, or correction to a previous registration.

Acknowledgements

When an MSB files its RMSB electronically, E-Filing immediately sends back an electronic confirmation of submission. Within two business days, the MSB also receives an electronic acknowledgement that its RMSB has been processed successfully. The acknowledgement includes the same Document Control Number (DCN) found on the paper letter subsequently sent to the MSB to officially acknowledge its registration with FinCEN. Because E-Filing reduces processing time, the MSB will receive its paper acknowledgement letter more quickly. While the paper acknowledgement letter currently represents an MSB's official proof of registration, FinCEN strongly encourages the MSB to save a copy of its E-Filing confirmation and acknowledgement notices. An MSB may use these copies to document the status of its registration filing with its bank, federal or state examiner, or internal auditor.

---

84. FinCEN operates a Regulatory Helpline that provides assistance for financial institutions seeking clarification of their BSA obligations and certain requirements under the USA PATRIOT Act. MSBs and other financial institutions with MSB-related questions should contact the Regulatory Helpline at 800-949-2732, Option 1.

85. See FIN 2006-G006, Registration and De-Registration of Money Services Businesses (February 3, 2006), (http://www.fincen.gov/financial_institutions/msb/pdf/msbregistration_de_registration.pdf); 31 CFR 1022.380(b)(2)-(4).

Corrections

An MSB may use E-Filing to file a correction to a previously submitted paper or electronic RMSB.[86] This feature is especially convenient for an MSB that has received the Agent Request Initiative letter from FinCEN and must file a corrected RMSB to indicate it does not have any agents.[87]

Learn more about the BSA E-Filing System

Greater use of E-Filing assists FinCEN by more quickly providing law enforcement with important information relating to money laundering, terrorist financing and other financial crimes. MSBs should visit FinCEN's BSA E-Filing Web site to sign up and "Take a Tour" of the system.[88] MSBs also should review the E-Filing Brochure[89] and recent E-Filing webinar materials[90] for more information about the benefits of electronically filing the RMSB and other BSA reports. MSBs can contact FinCEN's BSA E-Filing Helpdesk with other questions specific to E-Filing.[91]

For clarification on regulatory requirements, including those established through the new final rules updating the definition of an MSB and establishing the regulatory requirements for prepaid access providers and sellers, MSBs should visit the MSB portion of FinCEN's website.[92] Further questions should be directed to FinCEN's Regulatory Helpline. Inquiries regarding RMSB acknowledgement letters, registration status, and DCNs currently should be directed to the Internal Revenue Service (IRS) Enterprise Computing Center-Detroit.[93]

---

86. For more information on how to file corrections, please see "Questions and Answers, Electronically Filing Your Registration of Money Services Businesses (RMSB) Form," http://www.fincen.gov/financial_institutions/msb/pdf/FAQ_E-Filing_RMSB_Outreach.pdf
87. See http://www.fincen.gov/financial_institutions/msb/agentrequest.html.
88. See http://bsaefiling.fincen.treas.gov/.
89. See http://www.fincen.gov/whatsnew/pdf/E-File_Brochure.pdf.
90. See http://www.fincen.gov/financial_institutions/msb/pdf/The-Benefits-of-BSA-E-Filing-In-Focus-MSB.pdf.
91. The E-Filing Helpdesk may be contacted at 866-346-9478, Option 1 or via e-mail at BSAEfilingHelp@fincen.gov.
92. See http://www.fincen.gov/financial_institutions/msb.
93. The IRS Enterprise Computing Center-Detroit may be contacted at 866-270-0733.

Distinguishing Between Bank Secrecy Act SARs and National Suspicious Activity Reporting Initiatives

By FinCEN's Office of Outreach Resources

Efforts to identify and report suspicious activity have increased in the 10 years since the terrorist attacks of September 11, 2001 and reporting suspicious activity is nothing new to financial institutions that have a SAR reporting requirement under FinCEN's regulations implementing the BSA. However, these SARs are not the only suspicious activity reporting mechanism in the national effort to identify and report potential criminal or terrorism-related activity.

Likewise, suspicious activity is not limited to financial transactions. It can occur at any time or place, and there are a number of tools available for the reporting of such activity and the sharing of information once reported. FinCEN would like to highlight two of the more widely known efforts and remind filers that these initiatives are separate and distinct from SAR requirements under the BSA.

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), a partnership of local, state, tribal and federal agencies, was created to provide a means by which law enforcement professionals at all levels can share information about suspicious activity that is potentially terrorism-related. Led by the Department of Justice, the NSI facilitates the "gathering, documenting, processing, analyzing and sharing"[94] of suspicious activity reported through this initiative. As part of this effort, participating organizations have developed training for law enforcement professionals in recognizing potential terrorism-related activity. Further information regarding the NSI is available at http://nsi.ncirc.gov/. Additional information is also available in NSI's 2010 Annual Report.

Launched in conjunction with NSI, an initiative available to the general public for reporting suspicious activity that they may observe is the Department of Homeland Security (DHS)'s national "If You See Something, Say Something™" public awareness campaign. This campaign aims to raise the awareness of the general public of potential terrorism-related or other suspicious activity that may threaten

94. http://nsi.ncirc.gov/

homeland security, and the importance of reporting such activity to the authorities. Further information regarding DHS's "If You See Something, Say Something™" campaign is available at http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm.

Law enforcement agencies may utilize BSA data in investigations related to either of these initiatives, or any other effort to identify suspicious activity or potential terrorism-related activities. However, these initiatives are distinctly different from the requirement financial institutions have to file a SAR to report suspicious transactions that are conducted or attempted by, at or through their institution. Financial institutions should continue to report transactions they determine to be suspicious in nature by completing and filing with FinCEN the appropriate SAR form.

For questions regarding SAR requirements under the BSA, please contact FinCEN's Regulatory Helpline at 800-949-2732.

Section 5 — Industry Forum

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into an aspect of compliance management or fraud prevention. In this issue, Michael Reiss of the International Precious Metals Institute offers his insights into the money laundering risks associated with trading cash for gold. 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.

Cash for Gold: Where the Rubber Meets the Road

By Michael Reiss, representing the International Precious Metals Institute on the Bank Secrecy Act Advisory Group

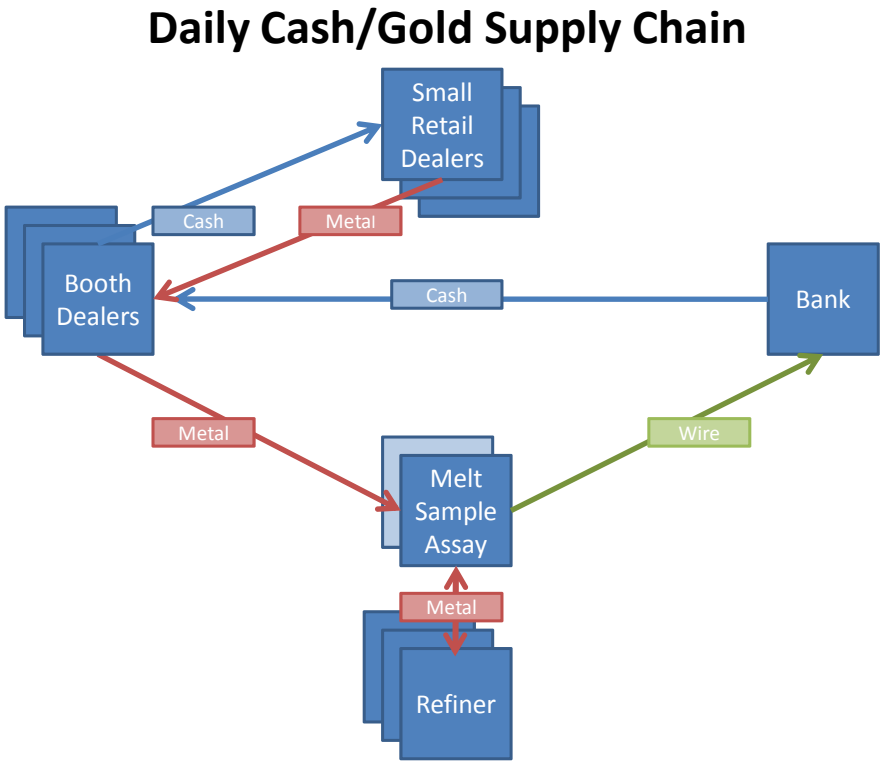
Jewelry stores, coin dealers, airport kiosks, antique shops—it seems everyone wants to help you raise cash for your old jewelry. How likely is it that you will be dealing with a money-launderer?

At first glance, not very. Transactions typically run from $100 to $500. A $2000 sale at a gold party would probably be the biggest of the day even at today's prices. But at close of business, a gold buyer might well disburse $50,000 in cash for gold jewelry. If the buyer sells the gold and is paid by check, placement is a possibility. More likely, the sale will be for cash.

Is the retail cash-for-gold business suspicious? Scams associated with the retail business have drawn considerable attention, but not necessarily for laundering. Retail scrap jewelry sales is a small subset of a much larger business that has attracted enforcement interest for decades, but with few results. Over the last 25 years, there have been only two noteworthy enforcement operations in the whole of the precious metals industry—Polar Cap from 1986 to 1992 and Meltdown in 2003. Both centered on jewelry districts and both involved precious metals in the form of scrap—but not the retail trade directly.

The jewelry districts throughout the country are the centers of this business. In these centers, thousands of dealers compete for gold scrap from offices and exchange booths. They are the crossroads where the visible business in gold—conducted by check or wire transfer—turns into invisible cash transactions. There is no bright line but the transition is discernable.

The retail gold buying business moves downstream through the supply chain roughly like this:



1. The small retail dealer buys gold from the public. He or she cannot tell visually how much gold is in a piece of jewelry, so will generally test for gold content. But the tests tend to be primitive, so to protect against inaccurate estimates of gold contained (and because sellers at the retail level are often unsophisticated) profit margins are high.

2. Dealers in jewelry exchange booths buy gold scrap from a small dealer—perhaps from the retail dealer that sponsored the gold buying party or a small precious metals scrap collector. The booth dealer tests the scrap to pinpoint the precious metals contained. Today, testing is with an x-ray fluorescence instrument; 20 years ago, it was with a stone and acid. Most payments to the

small dealers are by cash, so in most cases the small dealers are making no attempt to place currency into the financial system. For those being paid by check, placement is a possibility.

3. The booth dealer delivers the scrap to a melter who again weighs, samples and assays to confirm the precious metals content.

4. Based on the test results and the current gold price, the melter transfers funds the same day to the booth dealer's bank account. The melter is the critical point in this circuit, ironing wrinkles in the money transfer process and sometimes advancing payment to the booth dealer if there are delays.

5. The next morning, the bank delivers cash to the booth dealer's counter by armored truck—$50,000 to $500,000 a day or more— and the cycle begins again.

The cash that booth dealers receive from melters and pay to small dealers passes through a bank, so transactions are a matter of record. The melter could—and sometimes does—pay a booth dealer directly, in which case the audit trail might get fuzzy. However, melters at this level generally avoid doing cash transactions. The melters are the fulcrum of the business and, knowing they are in enforcement's crosshairs, they avoid the exposure of cash transactions. And since each melter deals with dozens of booth dealers, the cash needed to pay all the booth dealers with currency would pose a huge security problem.

Just to close the circle, at the bottom of the diagram, the melter delivers the scrap precious metal to a refiner. The refiner separates and refines the precious metals contained to elemental form—in the case of 14 karat jewelry, to gold, silver and perhaps some platinum or palladium. The refiner returns the precious metal to the melter, who sells it to consumers.

Generally, laundering at the placement stage has been by buying scrap precious metal for cash and selling it to a buyer that pays by check or wire. It is the extraordinarily low cost of converting scrap to fungible metal that makes scrap an attractive laundering vehicle. The cost of converting jewelry scrap to 99.99% pure gold is trivial and the business is intensely competitive. In the diagram, aggregate gross profits on jewelry scrap from the booth dealer through the refiner are less than 2% and payment is often within a day or two. The ultimate refining charge might be 1/4% or 1/2 % of the precious metals value. This is why historically scrap has been the launderers' grade of choice.

Conversely, even though laundering in precious metals has centered in jewelry districts, jewelry and other manufactured items containing gold are seldom used for laundering. If a product goes out of style or becomes obsolete or is defective, as a practical matter, it is scrap. Why pay and risk losing the manufacturing value added when one can deal in scrap from the outset?

Section 6 – Feedback Form

Financial Crimes Enforcement Network

U.S. Department of the Treasury

Tell Us What You Think

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

Questions regarding *The SAR Activity Review* can be submitted to sar.review@fincen.gov. For all other questions, please contact our Regulatory Helpline at 1-800-949-2732. **Please do not submit questions regarding suspicious activity reports to the SAR Activity Review mailbox.**

A. Please identify your type of financial institution.

Depository Institution:
__ Bank or Bank Holding Company
__ Savings Association
__ Credit Union
__ Foreign Bank with U.S. Branches or Agencies

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

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

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

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

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

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

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

_____
_____
_____
_____

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

_____
_____
_____
_____

E. What new TOPICS, TRENDS, or PATTERNS in suspicious activity would you like to see addressed in the next edition of The SAR Activity Review – Trends, Tips & Issues? Please be specific, for example: information on a certain type of activity, or an emerging technology of interest.

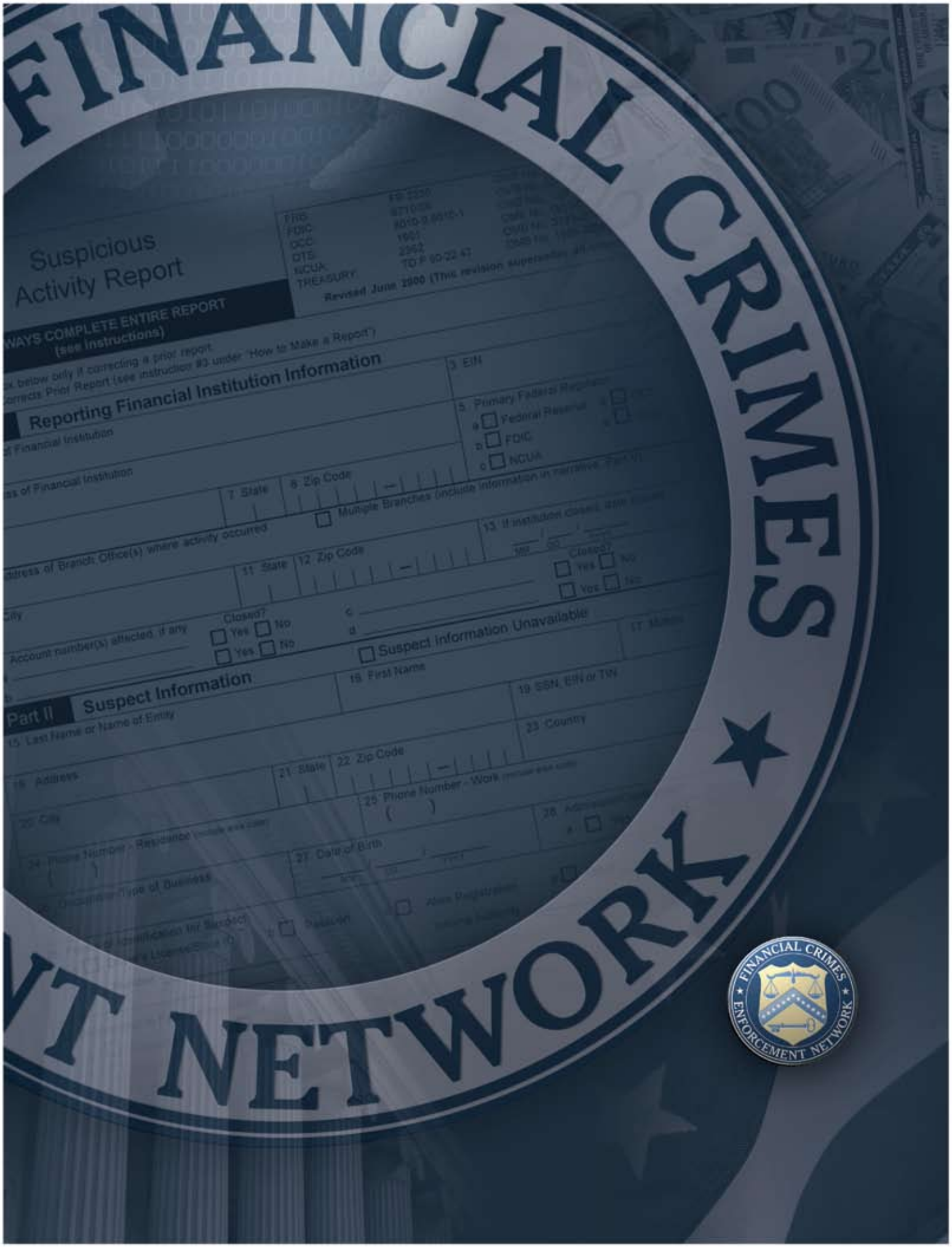
_____
_____
_____
_____

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

_____
_____
_____
_____

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

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


FINANCIAL CRIMES
NETWORK
Suspicious
Activity Report
Revised June 2000 (This revision supersedes all
WAYS COMPLETE ENTIRE REPORT
(see instructions)
Reporting Financial Institution Information
Suspect Information
Suspect Information Unavailable
FINANCIAL CRIMES
ENFORCEMENT NETWORK