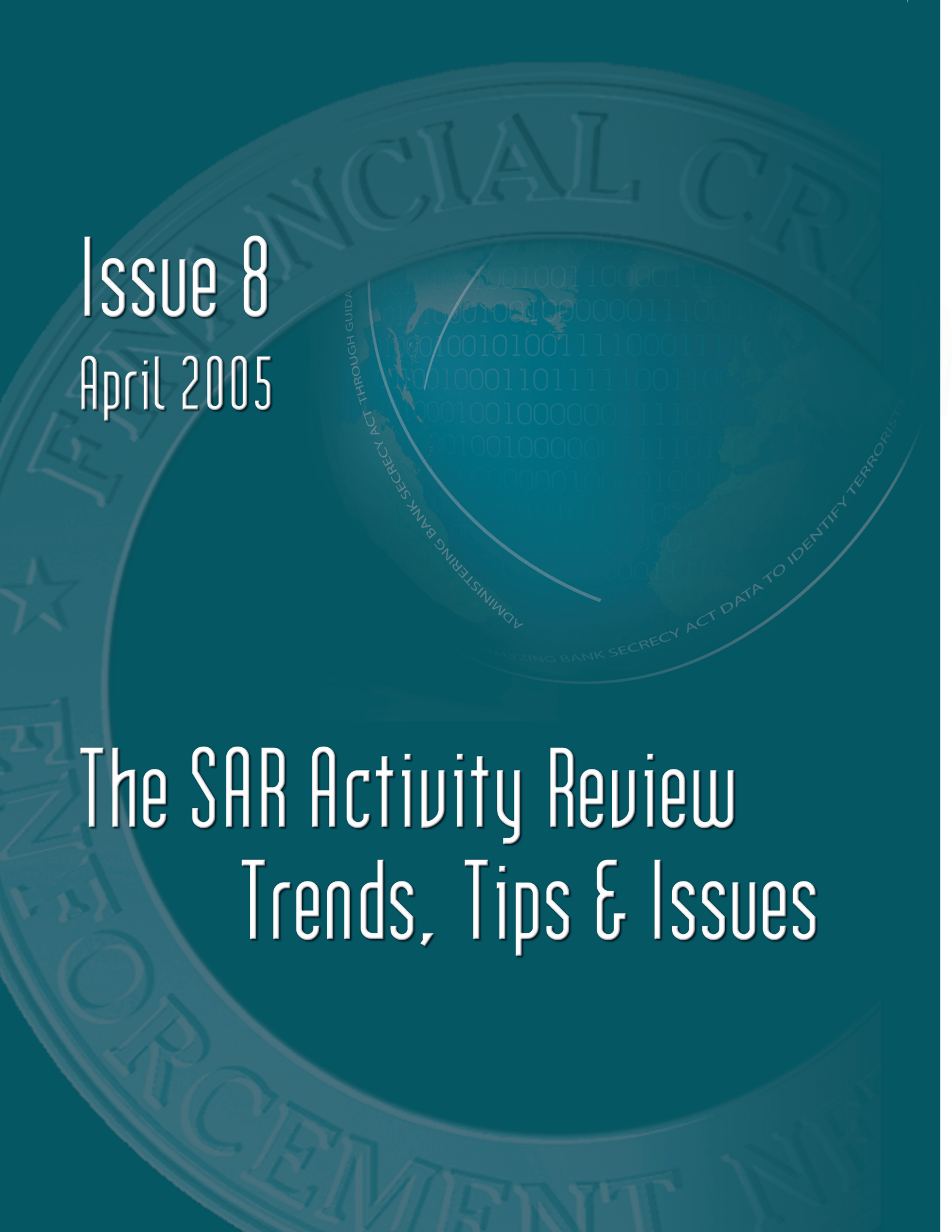
Issue 8

April 2005



The SAR Activity Review
Trends, Tips & Issues

The SAR Activity Review

Trends Tips & Issues

Issue 8

Published under the auspices of the Bank Secrecy Act Advisory Group

April 2005

Table of Contents

Introduction……..…….……....…….....…….....1

Section 1 – Director's Forum…….……..3

Section 2 - Trends and Analysis

Terrorist Financing Suspicious Activity Reports .....…….....5

Suspicious Activity Report Filings within the Casino and
Card Club Industries.....19

Section 3 - Law Enforcement Cases

Investigations Assisted by Suspicious Activity Reports .....……..25

Section 4 - Tips on Suspicious Activity Report Form Preparation & Filing

Suspicious Activity Report Form Completion Tips – A trend analysis
of frequently asked questions received on FinCEN's
Regulatory Helpline.....……..……29

Section 5 - Issues & Guidance

National Security Letters and Suspicious Activity Reporting…….....35

Revised Guidance on Filing Suspicious Activity Reports Relating to
the Office of Foreign Assets Control *List of Specially Designated
Nationals and Blocked Persons*……..…….....38

Suspicious Activity Involving the Iraqi Dinar…….....41

Section 6 - Industry Forum

An Overview of Suspicious Activity Report Training Elements in 2005….....43

Section 7 - Feedback Form…….47

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

Introduction

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

The year 2005 marks another exciting change for *The SAR Activity Review-Trends, Tips & Issues*. The redesigned publication will now contain a shortened Trends and Analysis section, which will address one topic of interest to depository institutions and another topic of interest to one of the other regulated industries. A newly added section provides FinCEN's Director, William J. Fox, the opportunity to address current, significant issues. This revised format will be published three times annually.

This edition features:

- Section 1, Director's Forum.
- Section 2, Trends and Analysis - Suspicious Activity Reports related to terrorist financing and Suspicious Activity Report filing trends in one facet of the casino and card club industry.
- Section 3, Law Enforcement Cases - summaries of Suspicious Activity Reports used in criminal investigations.
- Sections 4, Tips on Suspicious Activity Report Form Preparation and Filing - guidance for financial institutions on filing Suspicious Activity Reports involving multiple suspects; victims of suspicious activity; unavailable suspect information; and correcting and updating previously filed Suspicious Activity Reports.

---

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

- Section 5, Issues and Guidance - revised guidance for filing Suspicious Activity Reports when also reporting under the Office of Foreign Assets Control *List of Specially Designated Nationals and Blocked Persons*; guidance for Suspicious Activity Report filings related to National Security Letters; and guidance in reporting suspicious activity involving the Iraqi dinar.

- Section 6, Industry Forum - insight from one of our industry partners about Suspicious Activity Report training.

- Section 7, Feedback form.

Your comments and feedback are important to us. Please take a moment and let us know if the topics chosen are helpful and if our new publication process is beneficial. We have included a feedback sheet in Section 7. Your comments may be addressed to either or both of *The SAR Activity Review* project co-chairs:

John J. Byrne
Director
ABA Center for Regulatory Compliance
American Bankers Association
1120 Connecticut Ave., NW
Washington, DC 20036
(202) 663-5029 (phone)
1-800-BANKERS
(202) 828-5052 (fax)
jbyrne@aba.com

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

Section 1 - Director's Forum

The eighth edition of *The SAR Activity Review* comes at a time of unprecedented anxiety in the financial community over Bank Secrecy Act compliance expectations generally, and the filing of Suspicious Activity Reports in particular. Such anxiety is not without foundation and has not gone unnoticed by regulators and policymakers.

With respect to the filing of Suspicious Activity Reports, at risk is the quality of the information reported. The Financial Crimes Enforcement Network is the largest overt collector of financial intelligence in the United States, if not the world. We are responsible for ensuring the collection, analysis, and dissemination of information collected under the Bank Secrecy Act, including, most notably, the Suspicious Activity Report. These reports serve not only to provide law enforcement, intelligence, and regulatory agencies with leads indicative of illicit activity, but also to provide a fertile source for identifying trends and patterns of illicit activity as well as compliance-related deficiencies.

We estimate that if current filing trends continue, the total number of Suspicious Activity Reports filed this year will far surpass those filed in previous years. While the volume of filings alone may not reveal a problem, it fuels our concern that financial institutions are becoming increasingly convinced that the key to avoiding regulatory and criminal scrutiny under the Bank Secrecy Act is to file more reports, regardless of whether the conduct or transaction identified is suspicious. These "defensive filings" populate our database with reports that have little value, degrade the valuable reports in the database and implicate privacy concerns. Financial institutions from the smallest community banks and credit unions to the largest international banks are telling us that they would rather file than face potential criticism after the fact.

If this trend continues, consumers of the data – law enforcement, regulatory agencies, and intelligence agencies – will suffer. While the most sophisticated of analytical tools and data warehouses allow users to more efficiently exploit the data, no system can effectively cull defensively filed reports.

Without a review of underlying supporting documentation, it is often impossible to detect those Suspicious Activity Reports that relate to activity that is not in fact suspicious.

It is no great insight to conclude that the conception of a single, clear policy on suspicious activity reporting combined with consistency in the application of that policy is the solution to the defensive filing phenomenon. Yet such consistency continues to be elusive. Together with our partners in the federal regulatory agencies and law enforcement, we are working to ensure clear, unified Bank Secrecy Act policy that all stakeholder agencies apply consistently. However, we do not stop there. For example, in recognition of the invaluable role played by state-based financial regulators, and thanks in large part to the work of the Conference of State Bank Supervisors, we have recently completed a model information sharing agreement that would facilitate the flow of information between FinCEN and the state regulators. Such an agreement would enhance the efficiency of both the state regulators as well as FinCEN, and would be another significant step toward ensuring greater consistency in the application of the Bank Secrecy Act. We will be reaching out shortly to the states to discuss this model agreement and look forward to furthering our working relationships with them.

Addressing the defensive filing phenomenon, like the other important Bank Secrecy Act compliance issues, is the collective responsibility not only of the Department of the Treasury and FinCEN, but also of the many federal and state regulatory and law enforcement agencies involved with the administration of the Act. I reaffirm my pledge to continue to work closely with the industry and all others to ensure the consistent application of the suspicious activity reporting regulation.

William J. Fox
Director, Financial Crimes
Enforcement Network

Section 2 - Trends and Analysis

This section of *The SAR Activity Review-Trends, Tips & Issues* provides examples and patterns identified in suspicious activity reporting by both depository and non-depository institutions. This edition will address Suspicious Activity Reports related to terrorist financing as well as filing patterns and trends related to the casino and card club industry.

Terrorist Financing Suspicious Activity Reports

FinCEN continually monitors the Suspicious Activity Report database and examines the extent to which Suspicious Activity Reports have been filed by institutions that suspect terrorism or terrorist financing. Previous issues of *The SAR Activity Review* provided financial institutions with examples of terrorist financing to help them identify and report suspicious activity.[2] A recent analysis of Suspicious Activity Reports filed between April 1, 2003 and June 30, 2004, identified 2,175 Suspicious Activity Reports submitted to FinCEN by depository institutions, casinos, money services businesses, and the securities and futures industries related to possible terrorist financing.[3]

The following sections provide an in-depth analysis of terrorist financing filing trends found in those reports by examining geography, violation amounts, suspicious activity patterns, and the types of fund transfers involved.

Filing Trends

The number of Suspicious Activity Reports for suspected terrorist financing declined immediately after the events of September 11, 2001 and the fourth quarter of that year, but began increasing in the second quarter of 2003. The increase can partially be attributed to the additional number of financial institutions now required to file Suspicious Activity Reports, e.g., money services businesses, casinos, and securities and futures industries. The increase

[2] For additional information, see Issue 4, pages 17-19 (http://www.fincen.gov/sarreview082002.pdf); Issue 5, pages 19-21 (http://www.fincen.gov/sarreviewissue5.pdf); and Issue 6, page 3 (http://www.fincen.gov/sarreviewissue6.pdf.)

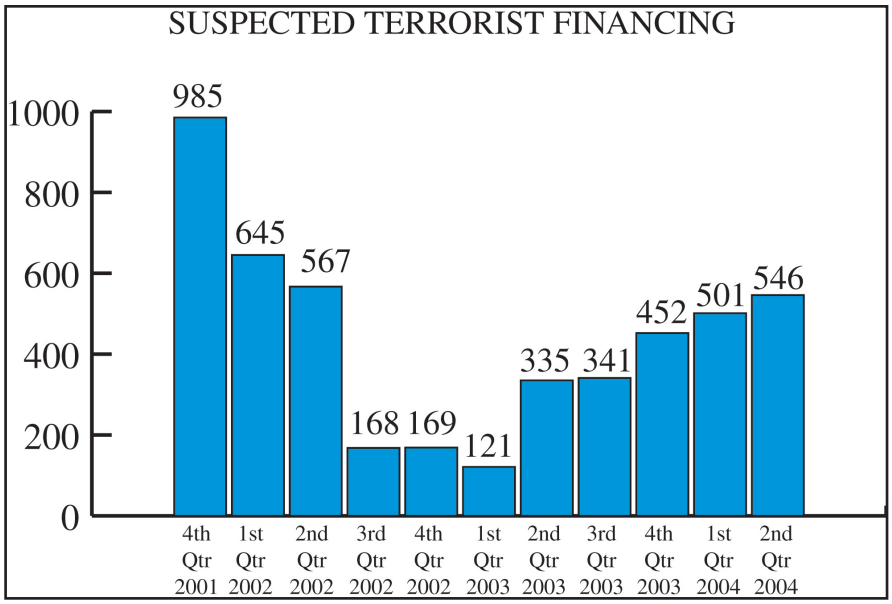
[3] Search criteria during this study included searches on the suspicious activity code specifically designated for suspected Terrorist Financing, and keyword searches where the suspicious activity code was designated as "Other" and Narrative fields for the following search terms: all forms of the word "terror," September 11(th), 9/11, 9/11/01, World Trade Center, WTC, Pentagon, Control List, Watch List, Hijacking(s) and Hijacker.

in filings reporting terrorist financing also coincides with the war in Iraq and continuing terrorist attacks around the globe. According to the United States Department of State *Patterns of Global Terrorism 2003 Report (Revised)*, there was a slight increase in the number of international terrorist attacks during this period, rising from 198 in 2002 to 208 in 2003. Another possible explanation for the increase in reports of terrorist financing activity may be the publicity surrounding the investigations of some financial institutions with customers and transactions with possible ties to terrorism.

Among the types of terrorist financing reported, Suspicious Activity Report filers identified activity that was previously described by FinCEN as possibly indicating terrorist financing in the January 2002 SAR Bulletin Issue No. 4, "Aspects of Financial Transactions Indicative of Terrorist Financing."[4] For example, 4% of the 2,175 Suspicious Activity Report filings recently reviewed involved charities suspected of terrorist financing. Other activities reported include: a customer who appeared to be purchasing maps and books with information on bridge construction; a customer seen taking pictures of internal structural designs at one financial establishment; and a letter intended for the President of the United States, but mailed to the bank filing the report (the author of the letter claimed to know the identity of a September 11th terrorist). The financial institutions that filed these Suspicious Activity Reports also directly contacted law enforcement agencies to report the suspicious activities.

The following chart depicts the trend in filings of the 4,830 terrorist-financing-related Suspicious Activity Reports filed since October 2001:

[4] See SAR Bulletin 4 at http://www.fincen.gov/sarbul0201-f.pdf.



Terrorist Financing Suspicious Activity Reports by Industry

Depository Institution Industry: Suspicious Activity Reports by Depository Institutions

Of the 2,175 Suspicious Activity Reports filed during the review period related to terrorist financing, 1,014 of the Suspicious Activity Reports were filed by 177 depository institutions in 46 states, Puerto Rico, Guam and the United Kingdom. Significantly, two depository institutions were responsible for filing 38% of those Suspicious Activity Reports; both institutions filed comprehensive, proactive reports that clearly articulated the factual basis for suspecting illegal activity.[5] Out of the 1,014 depository institution Suspicious Activity Reports, only 4 reports did not contain a written narrative.

[5] The term "proactive" refers to acting in advance or being anticipatory. As opposed to "reactive" reporting which occurs when a financial institution files a report due to information obtained from law enforcement, news sources, bulletins and other sources.

Money Services Business Industry: Suspicious Activity Reports by Money Services Businesses

A total of 334 money services businesses in 42 states, Puerto Rico, and the Dominican Republic filed 1,116 Suspicious Activity Reports that identified terrorist financing as the category of suspicious activity.

Securities and Futures Industry: Suspicious Activity Reports by Securities and Futures Industries

A total of 19 institutions within the securities and futures industries in 11 states filed 31 Suspicious Activity Reports related to possible terrorist financing. Broker-dealers located in New York and Florida filed 45% of those reports.

Casino Industry: Suspicious Activity Report by Casinos and Card Clubs

This study identified 14 terrorist-financing-related Suspicious Activity Reports by Casinos and Card Clubs. One casino filed 11 of the reports covering a series of fraudulent checks involving an individual from the Middle East.

Filer Locations

The following table lists the top ten states where financial institutions' Terrorist Financing Suspicious Activity Report filings originated:

Terrorist Financing Suspicious Activity Reports: April 2003-June 2004
Suspicious Activity Reports Filed by Financial Institutions in the Top Ten States

Filer State	*Depository Institutions*	*Money Services Businesses*	*Casinos*	*Securities/ Futures*	*Total*
NY	322	129	0	10	**461**
CA	45	163	0	3	**211**
NJ	92	17	0	1	**110**
FL	66	34	0	4	**104**
PA	74	17	0	0	**91**
VA	75	13	0	0	**88**
MA	45	24	0	1	**70**
IL	17	34	0	1	**52**
TX	17	23	0	0	**40**
GA	31	8	0	0	**39**

Suspect Location

Within the United States

The following table lists the top ten states in which the suspects resided:

Terrorist Financing Suspicious Activity Reports: April 2003-June 2004
Suspect's Residence State

Suspect State	*Depository Institutions*	*Money Services Businesses*	*Casinos*	*Securities/ Futures*	*Total*
NY	251	131	1	1	**384**
CA	34	80	2	3	**119**
FL	66	47	0	2	**115**
NJ	88	18	0	0	**106**
VA	80	18	0	2	**100**
PA	50	25	0	0	**75**
MA	38	28	0	1	**67**
TX	23	29	0	3	**55**
IL	14	29	1	1	**45**
GA	28	12	0	0	**40**
Total	**672**	**417**	**4**	**14**	**1106**

Outside the United States

Suspicious Activity Reports filed by depository institutions, the securities and futures industries, and money services businesses reported that nearly 4% of the suspects lived in foreign countries. The following chart depicts the geographic regions where the reported suspects resided:

Terrorist Financing Suspicious Activity Reports: April 2003-June 2004
Foreign Suspect Residences

REGION	*Depository Institutions*	*Securities/Futures*	*Money Services Businesses*	*Total*
MIDDLE EAST[6]	25	5	0	**30**
EUROPE[7]	13	0	2	**15**
ASIA[8]	7	0	5	**12**
AFRICA[9]	3	2	2	**7**
NORTH AMERICA[10]	2	0	5	**7**
CARIBBEAN[11]	1	0	1	**2**
CENTRAL AMERICA[12]	1	3	0	**4**
SOUTH AMERICA[13]	2	0	0	**2**
Total	**54**	**10**	**15**	**79**

[6] Egypt, Iraq, Jordan, Kuwait, Lebanon, Saudi Arabia, Syria and United Arab Emirates.
[7] Austria, Germany, Italy, Norway, Spain, Turkey, and the United Kingdom.
[8] China, Indonesia, Pakistan, Philippines, Singapore and Vietnam.
[9] Côte d'Ivoire, Ethiopia, Ghana, Mauritania, Nigeria, and South Africa.
[10] Canada and Mexico.
[11] Dominican Republic and Jamaica.
[12] Panama.
[13] Paraguay and Venezuela.

Violation Amounts Reported

The violation amounts reported in terrorist-financing-related Suspicious Activity Reports ranged from $0 to $500 million. Of these Suspicious Activity Reports, some of the higher violation amounts included:

- A Suspicious Activity Report involving nearly $500 million identified an individual associated with an organization known to provide funds to terrorist organizations.

- A Suspicious Activity Report described numerous wire transfers totaling more than $200 million conducted by a textile business. The beneficiaries of the wires were businesses that appeared to be inconsistent with the originator's stated business.

- A Suspicious Activity Report involving more than $3 million was filed after the institution was advised by law enforcement that the suspect had been indicted for money laundering.

The following table illustrates the violation amounts cited on all terrorist-financing-related Suspicious Activity Reports:

Terrorist Financing Suspicious Activity Reports: April 2003-June 2004
Reported Violation Amounts

Violation Amount	*Depository Institutions*	*Money Services Businesses*	*Casinos*	*Securities/Futures*	*Total*
$0	124	140	2	15	**281**
$1 - $10,000	154	832	4	2	**992**
$10,001 - $100,000	384	136	6	6	**532**
$100,001 - $500,000	211	6	1	3	**221**
$500,001 - $1,000,000	48	1	1	0	**50**
>$1,000,000	93	1	0	5	**99**
Total	**1014**	**1116**	**14**	**31**	**2175**

Suspicious Activity Patterns

Depository Institutions

This study confirmed a significant increase in proactive Suspicious Activity Report filings. Twenty percent of depository institutions' Suspicious Activity Reports were filed in response to law enforcement inquiries, name matches with the Office of Foreign Assets Control *List of Specially Designated Nationals and Blocked Persons*, and/or news articles; the remaining eighty percent were proactive. This proactive filing trend is in contrast to the 75% to 80%

rate of reactive Suspicious Activity Report filings that occurred immediately after September 11, 2001. When Suspicious Activity Reports were filed as a result of a law enforcement inquiry, filers continued monitoring the targeted customer's account(s) after the initial requested information was provided. Any suspicious activity subsequent to the initial report was provided in supplemental Suspicious Activity Reports. The follow-up reports named additional suspects that had been linked by transactions or addresses to the original suspects as well as information identified in public databases. Some depository institutions also reported the methodologies routinely used to monitor customer and correspondent account activities, especially transactions involving foreign countries with known links to terrorism.

An example of proactive reporting by one depository institution described the following activity:
The institution filed seven reports on seven different individuals with Middle Eastern names suspected of being involved in a credit card bust-out scheme. Each report described how the perpetrator opened a credit card account, used it to the maximum credit limit, made a fraudulent payment, and then conducted additional charges to the credit limit before the payment was returned as uncollectible. The types of charges made during the "bust-out" phase were for cash advances, jewelry, airline tickets, and cigarettes. One individual used the credit card to pay federal income taxes during the bust-out phase.

Money Services Businesses

The most common activities reported in the 1,116 Suspicious Activity Reports by Money Services Business filings were structuring and smurfing.[14] Structuring was reported in over half of these reports; however, many reports did not include any narrative description of the transaction. Approximately 97 money services businesses reported a pattern of individuals using straw parties[15] or false identifications to wire funds to evade the identification requirement. Eight percent of the Suspicious Activity Report by Money Services Business filings involved Middle Eastern countries. A check cashing business filed approximately one-third of those reports.

---

[14] Smurfing is defined as the use of two or more persons to conduct related financial transactions, which could have been completed in a single transaction. The purpose is to avoid the reporting requirements of the Bank Secrecy Act that would be necessary if a single transaction were conducted.
[15] In this activity, an individual (the "straw party") conducts a wire transmittal at a money services business. Although the "straw party" participates in the transaction, he/she may not know its purpose or realize that they are assisting the originator in criminal activity.

The following bullets are examples of the types of activity reported in proactive Suspicious Activity Reports received from money services businesses:

- The sales/purchases through the Internet of substances that have routine lab uses and are also used as components of nuclear fusion weapons or hydrogen bombs. Buyers of this substance also purchased military or law enforcement equipment.
- The sale of a chemical compound used in the production of an illegal drug. The same purchaser also acquired items that could be used for illegal or terrorist purposes.

Securities and Futures Industries

Although the number of filings related to terrorist financing for the securities and futures industries was small (a total of 31 Suspicious Activity Reports from April 1, 2003 through June 30, 2004), some recognizable patterns were observed in the reports.

- 32% were filed because of links to the Office of Foreign Assets Control *List of Specially Designated Nationals and Blocked Persons* or Law Enforcement requests for information;
- 26% were filed as a result of continuing due diligence on existing accounts; the customer's name appeared in a news article; and
- 10% described attempted Nigerian Advance Fee Fraud schemes.[16]

Casinos and Card Clubs

There were two discernable patterns identified in Suspicious Activity Reports by Casinos and Card Clubs:

1. Casino filers appeared to classify the suspicious activity as terrorist financing when the suspect named in the Suspicious Activity Report was in some way connected to the Middle East, i.e., suspect name or nationality. For example, reports were filed because the activity involved fraudulent checks from the Middle East, the suspects had Arabic sounding names, or reports were

[16]In the "Advance Fee Fraud" schemes or 4-1-9 (a section of the Nigerian penal law that prohibits this activity), victims may receive emails and letters from groups of con artists, located in Nigeria, who claim to have access to a very large sum of money and want to use the victim's bank account to transfer the funds. In exchange for the victim's services, they claim they will give the recipient of the email/letter a large percentage of the funds. The con artists usually request that they be furnished with blank company letterhead, and/or bank account information. In Issue 7 of *The SAR Activity Review,* pages 47-48, FinCEN instructed financial institutions not to file Suspicious Activity Reports on advance fee fraud schemes unless such schemes involve a monetary loss.

filed when an expired Middle Eastern passport was presented for identification.

2. A few terrorist-financing-related Suspicious Activity Reports involved money transmitting services that some casinos provide. One report was filed when the casino was advised by a money services business that the casino was attempting to send funds to a person whose name appeared on the Office of Foreign Assets Control *List of Specially Designated Nationals and Blocked Persons*. Other Suspicious Activity Reports described suspected money-laundering schemes and possible terrorist financing indicated by incoming and outgoing wire transfers to multiple foreign locations.

Following are some examples of activities casinos suspected were terrorist-financing-related. In all of the instances described, the casinos directly contacted federal and state law enforcement to report the activities.

- A casino filed 11 Suspicious Activity Reports detailing instances of check fraud (including counterfeit checks) and possible terrorist financing involving an individual who was reportedly located in the Middle East. Research identified 9 Suspicious Activity Reports filed by depository institutions related to the same individual. The depository institutions' Suspicious Activity Reports identified possible Internet fraud, online automobile purchases, and aspects of a 419 Nigerian letter scheme.[17] None of the depository institutions identified these occurrences as terrorist financing. Instead, the depository institutions reported the activity as instances of check fraud, counterfeit check, and Internet fraud activity.

- One casino identified several individuals with New York and Illinois addresses suspected of minimal casino play[18] and terrorist financing. Apparently, the individuals used credit cards to purchase numerous $100 gift certificates.

---

[17] The 419 Nigerian Letter Scheme is also known as the "Advance Fee Fraud" scheme. Please refer to footnote 16.

[18] "Minimal Casino Play" most commonly refers to situations in which individuals exchange large amounts of currency for casino chips, gamble for a small amount of time (usually less than thirty minutes), either lose a nominal amount of chips or make small bets in comparison to the buy-in and then immediately cash out their chips. This activity is conducted to make the cash appear as a legitimate source of income.

- One casino filed a Suspicious Activity Report on a subject who provided an expired Middle Eastern passport for identification. When the casino refused to accept the expired passport, the subject provided a valid passport from a different Middle Eastern country. The subject was also curious as to what would happen to his account if something happened to him.

- Another casino reported an individual's excessive use of the casino's wire transmittal system (i.e., wire transfers). The Suspicious Activity Report indicated the individual was acting as a broker to other individuals who wanted to convert funds into "stored value currencies and/or digital Web money." (Most individuals are not able to convert funds to Web currency and therefore must use an intermediary.) Once the money was converted, the funds were used for Internet purchases.

Overall Activities

The following table illustrates the activities, individuals, and organizations reported by the financial institutions:

Terrorist Financing Suspicious Activity Reports: April 2003-June 2004
Types of Activities, Individuals and Organizations Reported

Activity	*Depository Institutions*	*Money Services Businesses*	*Securities/ Futures*	*Casinos*	*Total* [19]
Automated Teller Machine (ATM) Usage	34	0	0	0	**34**
Aviation	10	2	0	0	**12**
Charities	92	3	1	0	**96**
Flight Students	7	2	0	0	**9**
Foreign Check/Debit Card Transactions	1	4	0	0	**5**
Foreign Check Negotiations	67	0	0	0	**67**
Foreign Nationals	176	115	3	12	**306**
Fraud	46	134	4	0	**184**
Frequent Address/Name Changes	21	36	0	0	**57**
Government Watch Lists	147	6	10	1	**164**
Incoming Wire Transfers	76	27	0	0	**103**
Persons Identified in Press Reports	58	1	6	0	**65**
Purchases of Military & High Tech Goods	17	6	1	0	**24**
Source of Funds Unknown	41	5	1	0	**47**
Student, Non-Aviation	21	10	2	0	**33**
Wires to Foreign Countries	255	267	0	0	**522**
Total	**1069**	**618**	**28**	**13**	**1728**

[19] The total number of activities listed in the chart does not match the total number of Suspicious Activity Reports reviewed because some reports did not provide enough information to determine the nature of the activity, and others provided information on more than one activity.

Types of Fund Transfers

Wire Transfers

Wire transfers to and/or from foreign countries were reported in 625 (or 28%) of the 2,175 terrorist-financing-related Suspicious Activity Reports. The wire transfers reported involved both personal and business accounts. Ninety-six depository institutions reported that personal accounts were used for wire transfers in suspicious transactions while money services business filings reported all wire transfers were paid for with cash. The following tables show the geographic regions of these wire transfers:

Terrorist Financing Suspicious Activity Reports: April 2003-June 2004
Outgoing Wire Transfers

Region	*Depository Institutions*	*Money Services Businesses*	*TOTAL*
Africa	8	29	**37**
Asia	129	69	**198**
Australia/Oceania	2	0	**2**
Caribbean	3	10	**13**
Central America	0	11	**11**
Europe	56	32	**88**
Middle East	119	94	**213**
North America	15	14	**29**
South America	4	18	**22**
Total	**336**	**277**	**613**

Terrorist Financing Suspicious Activity Reports: April 2003-June 2004
Incoming Wire Transfers

Region	*Depository Institutions*	*Money Services Businesses*	*TOTAL*
Africa	1	1	**2**
Asia	11	3	**14**
Australia/Oceania	0	0	**0**
Caribbean	0	6	**6**
Central America	0	1	**1**
Europe	22	7	**29**
Middle East	46	13	**59**
North America	5	0	**5**
South America	2	1	**3**
Total	**87**	**32**	**119**

Automated Teller Machine (ATM) Transactions

Twenty-seven of the 1,014 depository institution terrorist-financing-related filings described activity involving funds deposited into bank accounts in the United States and then subsequently withdrawn using Automated Teller Machines located abroad; many involved personal accounts. A majority of the suspicious Automated Teller Machine withdrawals occurred in the Middle East (66%), with the remaining withdrawals in Europe (19%), Asia (11%) and North America (4%). The remaining seven Suspicious Activity Reports reporting this activity involved domestic, automated-teller-machine usage.

Checks

Sixty-seven, terrorist-financing-related Suspicious Activity Reports identified bank accounts held in the United States that had checks drawn on the accounts and negotiated in foreign countries; approximately one-third of those involved personal accounts. Some filers noted sequentially numbered checks and/or a signature on the check that did not match the handwriting used to fill in the payee and amount on the face of the checks. Some filers speculated that the account holder had signed blank checks and provided them to the ultimate user who later filled in payee and amount information. United States Customs and Border Protection inspectors have reported that signed blank checks are being transported out of the United States in order to avoid cross-border reporting requirements. Terrorist-financing-related Suspicious Activity Reports identified checks negotiated in Africa (2.8%), Asia (1.4%), Europe (1.4%), the Middle East (93%) and North America (1.4%).

What to Do if Terrorist Financing is Suspected

Financial institutions are reminded to report suspected terrorist financing by checking the appropriate box in the summary characterization, type or category of suspicious activity (depending on the form used by the particular financial industry), and to complete the Narrative (the most important section of the Suspicious Activity Report) by describing as completely as possible the potential terrorist-related or other suspicious activities, including an explanation about what makes the transactions suspicious. Significant information in the Narrative section, if available, includes any correspondent bank name/account information; names of cities, countries and foreign finan-

cial institutions linked to the transaction, especially if funds transfer activity is involved; and any account numbers and beneficiary names.

A Suspicious Activity Report should not be filed based solely on a person's ethnicity, nor should it be filed because a person appears to have the same name as individuals identified in the media as terrorists. Similarly, transactions to, from, or conducted by persons with possible affiliations with jurisdictions associated with terrorist activity should not be the only factor that prompts the filing of a Suspicious Activity Report. However, such information should prompt additional scrutiny of transactions and should be considered in conjunction with other relevant information in deciding whether a Suspicious Activity Report is warranted, as set forth in 31 CFR 103.18. For example, these factors combined with a lack of any apparent legal or business purpose to a transaction or a series of transactions could provide the basis for filing a Suspicious Activity Report. Resources that should be consulted about jurisdictions include: the U.S. Department of State *List of State Sponsors of Terrorism*; the Office of Foreign Assets Control *List of Specially Designated Nationals and Blocked Persons*; and the Financial Action Task Force *List of Non-Cooperative Countries and Territories*.[20]

[20] See Department of State *State Sponsors of Terrorism*: http://www.state.gov/s/ct/c14151.htm; Office of Foreign Assets Control *List of Specially Designated Nationals and Blocked Persons*: http://www.treas.gov/offices/enforcement/ofac/sdn/; Financial Action Task Force *List of Non-Cooperative Countries and Territories:* http://www1.oecd.org/fatf/NCCT_en.htm#List.

Suspicious Activity Report Filings Within the Casino and Card Club Industries

This section will discuss one facet of the casino industry, a particular type of casino referred to as racinos.

"Racinos"

"Racinos" generally are thought of as racetracks with slot machines. In practice, racetracks may be authorized by state law to engage in or offer a variety of collateral gaming operations, including slot machines, video lottery, video poker or card clubs. For example, subject to other applicable statutes and regulations, the Delaware State Lottery Office may license agents to operate video lottery machines within the confines of a racetrack licensed by the Delaware Thoroughbred Racing Commission.

The term "racino" has not been separately defined nor included specifically in the definition of casino for purposes of the Bank Secrecy Act. Instead, FinCEN relies on the state, territory or tribal characterization to determine whether an entity or operation will be classified as a casino for purposes of the Bank Secrecy Act. Therefore, if state law defines or characterizes slot machine operations at a racetrack as a "casino, gambling casino, or gaming establishment," and the gross annual gaming revenues of that operation exceed the $1 million threshold, then the operation would be deemed a "casino" for purposes of the Bank Secrecy Act.[21]

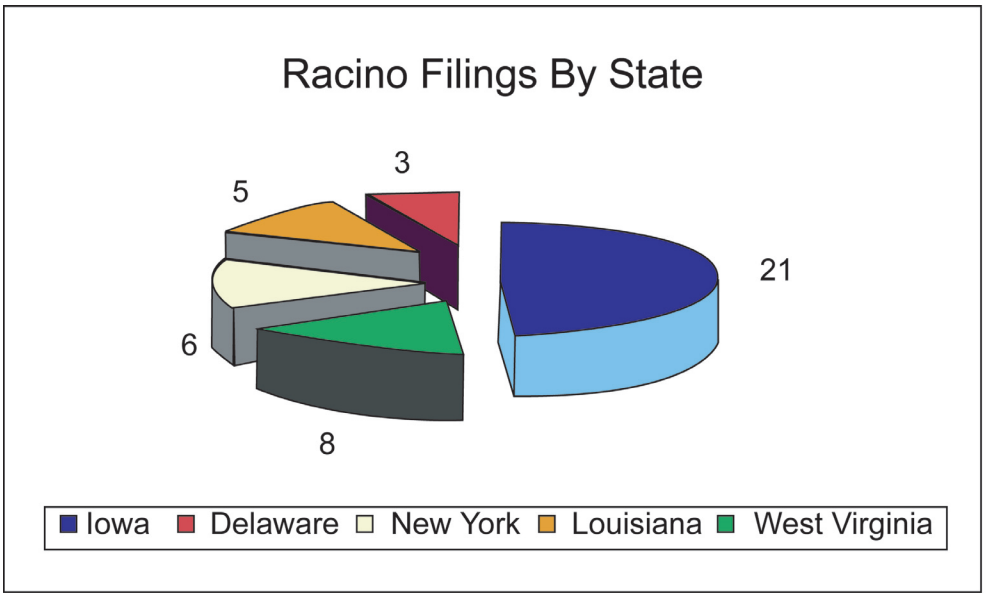
FinCEN has identified nine states that have authorized collateral gaming operations (such as those listed above) at racetracks: Delaware, Iowa, Louisiana, Maine, New Mexico, New York, Pennsylvania, Rhode Island, and West Virginia. Twenty-three "racinos" were identified operating in some of those nine states. It is estimated that approximately $2.66 billion was wagered at racinos in 2003.[22]

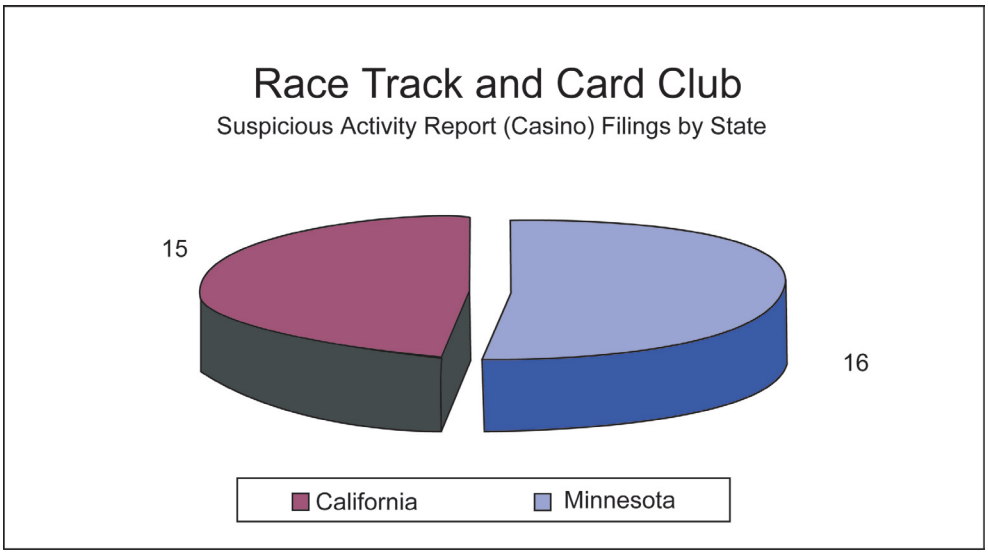
---

[21] In the United States, the casino industry is subject to a decentralized regulatory structure, primarily based on state/territory and tribal regulatory regimes. Under the Bank Secrecy Act and its implementing regulations, a gaming operation is defined as a financial institution subject to the requirements of the Bank Secrecy Act if it is a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 that is duly licensed as such under state law and authorized to do business in the United States, or is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act (other than certain social games for prizes of minimal value or traditional forms of Indian gaming engaged in by individuals as a part of, or in connection with, tribal ceremonies or celebrations).

[22] $812 billion was wagered at casinos and card clubs in 2003 (approximately 85 percent of the total amount of money wagered for all legal gaming activities throughout the U.S.). *See* Christiansen Capital Advisors, LLC, 2 Insight: Journal. Native. American. Gambling Industry. (Sept. 27, 2004).

For entities identified as "racinos," FinCEN queried the Bank Secrecy Act database for Suspicious Activity Reports filed from 1996 to September 30, 2004. Of the 14,060 Suspicious Activity Reports by Casinos and Card Clubs filed during that period, the query identified 74 reports filed by ten "racinos" and two racetracks with card clubs.[23] The following charts depict the twelve entities' filings by states.





[23] The class of gaming establishments known as "card clubs" was included in the definition of "casino" and thereby became subject to the requirements of the Bank Secrecy Act in 1998, see 63 FR 1919 (Jan.13, 1998).

Suspicious Activities Reported by "Racinos"

Currency exchange was one of the most frequently reported activities and was identified as suspicious in 16 reports, as follows:

- Exchanging small denominations of currency ($1s, $5s, $10s and $20s) for $100 bills (nine reports).
- Exchanging currency for casino chips or feeding currency into slot machines followed by cashing out with little or no gaming play (three reports).
- Exchanging large quantities of quarters from non-gaming proceeds for paper currency (three reports).[24]
- Customer requesting to add cash to casino winnings and then exchanging the combined cash and winnings for a single check issued by the casino.

Refusal to provide identification and use of false identification or Social Security numbers were identified in nine reports, as follows:

- Using false or multiple Social Security numbers (six reports).
- Refusing to provide required identification (two reports).
- Failure of one suspect to claim winnings totaling more than $30,000 over a three-year period claiming difficulty in obtaining a valid driver's license. The suspect did not produce any other type of identification, and provided a name that may have been false.

Racinos reported structuring, apparently for the purpose of avoiding reporting requirements, in six reports, as follows:

- Customers using agents to cash winnings (five reports).
- Customer requesting payment by three separate checks of $5,000 each (according to the customer it would be difficult to deposit a $15,000 check at the bank).

---

[24] The filer noted that one of the suspects was known to participate in criminal activity such as "skimming video game machines." This is a likely source of the quarters. "Skimming" can refer to schemes ranging from the removal of money from a machine prior to a count to complex schemes such as the theft of data through the use of a device attached to or placed on top of a video/Automated Teller Machine to capture passwords or account numbers from card magnetic strips or data keyed into the machine.

Fraud was reported in six reports, as follows:

- Tampering with the slot machines, causing them to pay out more winnings than they should have dispensed (three reports).
- A scam described as a "stringing" involving $100 bills in the self-service betting machines used at some racetracks to place bets (two reports). [25]
- Check alteration.

Suspicious Activities Reported by Racetracks with Card Clubs

Structuring was the most common activity reported by racetracks with card clubs. This activity was identified in eleven reports, as follows:

- Customers incrementally presented winnings for payout to avoid filing a Currency Transaction Report by a Casino (nine reports).[26]
- Two customers attempted to use agents to claim their winnings.
- One customer used multiple checks at different times to purchase casino chips in order to avoid the filing of a Currency Transaction Report by a Casino.

Refusal to provide identification and the use of false identification or Social Security numbers were identified in eleven reports, as follows:

- Customers refused to provide identification (seven reports).
- Customers using false identification (two reports).
- Customers using false Social Security numbers (two reports).

Money laundering was suspected when a customer deposited money with the casino and then cashed out without any play. This activity was identified in two reports.

---

[25] The term "stringing" refers to the practice of attaching a string or fishing line to a piece of currency (either coin or paper). The currency is inserted into a machine and pulled back to allow the machine to register the payment or play, and then pulled back before the machine collects the currency. In the reported filing, a team of individuals served as a lookout and blockers of video surveillance, during the stringing of a $100 bill in and out of a self-betting machine.

[26] One filer reported that they informed the customer he could return the following day to claim a portion of his winnings if he wanted to avoid the reporting requirement. Financial institutions are reminded that providing advice to customers on how to avoid the Currency Transaction Report filing requirements is a violation of 31 CFR 103.63(c).

The following fraudulent activities were also reported:

- Counterfeit currency used to purchase casino chips.
- Employee theft - A casino employee paid funds to an individual who had not played at the casino.

FinCEN continues to provide information to the regulated industries relevant to assessing risks facing the financial system, including information about trends and patterns that are being discovered. FinCEN has provided guidance to assist the casino industry in identifying transactions that may be considered "suspicious" for purposes of suspicious activity reporting through several means, including *The SAR Activity Review.*[27] FinCEN will continue to monitor the growth of "Racinos" and other types of gaming operations and will provide guidance or engage in additional rulemaking as appropriate.

[27] In December 2003, FinCEN issued "Suspicious Activity Reporting Guidance for Casinos," available at www.fincen.gov.

Section 3 – Law Enforcement Cases

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

Investigations Assisted by Suspicious Activity Reports

Suspicious Activity Report Initiates Material Support of Terrorism Investigation

The Federal Bureau of Investigation initiated a Material Support of Terrorism investigation based on a Suspicious Activity Report filed by a bank detailing a series of overseas financial transactions totaling millions of dollars. Two of the participants in these transactions were a United States based company and a money services business based in the Middle East. The bank was concerned by the unorthodox manner in which the transactions were executed and the disparate business operations of the participants. All of the money passed through an account held at the United States branch of a foreign bank headquartered in the Middle East.

During a seven month period millions of dollars passed through the money services business's bank account, immediately dispersing funds to scores of businesses and individuals around the world. Although the purpose of these payments is still under investigation, some of the recipients are known for, or suspected of, involvement in terrorist activities.
(Source: Federal Bureau of Investigation)

Purported Charity Attempts to Evade Reporting Requirements

Upon receipt of a Suspicious Activity Report from a bank, the Federal Bureau of Investigation initiated a bank and mail/wire fraud investigation involving a purported charity raising money for needy people in a Middle Eastern country. The Suspicious Activity Report identified a series of checks being deposited into an individual's personal checking account, all of which were just under $10,000. While this activity was not a violation of the Currency Transaction Reporting requirements, the activity was suspicious in nature to the bank. After several years of investigation, evidence was obtained indicating that the individuals involved did in fact know they were avoiding Internal Revenue Service scrutiny by moving money using checks written under the amount of $10,000. Seven individuals were charged with a variety of federal felonies including Money Laundering, Tax Fraud, Visa Fraud, Mail Fraud, and Wire Fraud. Four individuals pled guilty and are cooperating with the investigation. *(Source: Federal Bureau of Investigation)*

Retail Store Owner Sentenced For Unlicensed Hawala Operation

A retail store owner, who operated an unlicensed hawala (a form of an informal value transfer system), was sentenced to multiple months in prison and several years' probation. The defendant pled guilty to failure to register as a money services business as required by FinCEN and to filing a false tax return in connection with his failure to disclose his ownership of a foreign bank account. The defendant also agreed to forfeit several hundred thousand dollars in commissions and fees charged for the transfers.

The defendant operated a multi-million dollar money transfer business, which, at its peak, was transferring more than half a million dollars to a Middle Eastern country, out of the defendant's store. By the defendant's own admission, the individual transferred over $10 million to a Middle Eastern country through his hawala for over a year. The defendant did not have a state license and did not register with FinCEN. This investigation was initiated based on the filing of a Suspicious Activity Report.
(Source: Internal Revenue Service-Criminal Investigation)

Lengthy Sentence for Owning a Marijuana Farm

A defendant was sentenced to serve multiple months in prison followed by several years probation, after pleading guilty to narcotics trafficking charges and structuring financial transactions to evade the currency reporting requirements in connection with a marijuana growing operation. The defendant incorporated a business, falsely described in corporate documents as a real property development company, which the defendant then used to purchase acreage, set up the marijuana growing operation and hired people to run it.

According to the plea agreement, the defendant admitted to making over 100 cash deposits to the corporate account over several years. The cash deposits totaled more than $1 million, but each deposit was less than $10,000. This investigation was initiated based on the filing of a Suspicious Activity Report. *(Source: Internal Revenue Service-Criminal Investigation)*

Business Owner Sentenced for Tax Evasion

A business owner was sentenced to several years in prison followed by three years supervised release and ordered to pay a fine of nearly $1 million. The defendant was convicted of three counts of tax evasion and one count of structuring a financial transaction to avoid federal currency transaction reporting requirements. According to trial evidence, the defendant reported no taxable income and paid no federal income tax during three years, although the two businesses the defendant owned and operated were profitable and the defendant was earning a substantial taxable income from their operations. The defendant, an accountant by training, engaged in a complicated tax evasion scheme which involved diverting hundreds of thousands of dollars from the businesses into personal investment accounts held in the name of the defendant's spouse. The defendant created a phony shareholder loan account to make it appear that the corporations that owned the businesses owed the defendant money and then took false "bad debt" deductions on the defendant's own tax returns to offset the income earned personal investment accounts belonging to the defendant and the defendant's spouse. This investigation was initiated based on the filing of a Suspicious Activity Report. *(Source: Internal Revenue Service-Criminal Investigation)*

Insider Fraud Contributes to Bank Failure

The filing of a number of Suspicious Activity Reports resulted in an investigation by the Federal Bureau of Investigation of three individuals for their part in the failure of a community bank that had been in business since the early 1900s. The individuals, one of whom was an officer at the bank, allegedly engaged in a check-kiting conspiracy that caused the bank to lose several million dollars in the months preceding its failure. A multi-count indictment was returned against all three subjects. The charges include aiding and abetting misapplication of bank funds, conspiracy to misapply bank funds and to make false entries in the bank's financial records, wire fraud and making false entries in bank records. *(Source: Federal Bureau of Investigation)*

Money Remitting Business Laundering Drug Proceeds

A routine Suspicious Activity Report review by geographic zip codes led to the discovery of a retail store operator operating as a subagent for a licensed money services business. The preliminary investigation by the filing institution, along with a follow-up investigation by the Drug Enforcement Administration, led to the discovery that significantly more money was being remitted than the money services business customer base could generate. This ultimately resulted in a proactive investigation involving the use of court authorized wire-intercepts, wherein members of a violent street gang were discovered to be utilizing the remitting services of the target to move their drug proceeds both domestically and internationally.
(Source: Drug Enforcement Administration)

Business Used for Money Laundering and Pyramid Scheme

A Bureau of Immigration and Customs Enforcement's Bank Secrecy Act Enforcement Team received information that a business was a check cashing service, but the transactions within their bank accounts indicated that the business was involved in domestic money laundering and a pyramid fraud scheme. It was also learned that the business was attempting to withdraw a sizable amount of money from their accounts at two banks. The information was referred to the state's District Attorney's Office. With technical assistance from Immigration and Customs Enforcement, the District Attorney's Office froze the accounts and subsequently seized funds totaling more than $2.2 million. The main defendant pled guilty to committing securities and exchange fraud. *(Source: Immigration and Customs Enforcement)*

Section 4 – Tips on Suspicious Activity Report Form Preparation & Filing

Suspicious Activity Report Form Completion Tips – A trend analysis of frequently asked questions received on FinCEN's Regulatory Helpline

FinCEN has reviewed calls received on its Regulatory Helpline[28] from June to December 2004 for the most frequently asked questions about suspicious activity reporting. This article addresses the four most frequently asked questions received over the helpline about completing the Suspicious Activity Report form.[29] **Note:** These questions and answers will be separately posted to FinCEN's public website at www.fincen.gov.

1. Suspicious Activity Reports Involving Multiple Suspects

One of the most frequently asked Suspicious Activity Report form completion questions involves how to complete the form if there are multiple suspects. Suspicious activity often involves related transactions conducted by two or more persons. For example, different persons in a money-laundering network may make cash deposits structured below the reporting threshold. Although the financial institution may determine that each transaction constitutes a reportable suspicious activity, it may have knowledge or suspicion that the transactions are related. For example, currency may be deposited into the same account or a teller may have noticed multiple suspects arriving in the same automobile.

If a financial institution wishes to report suspicious activity involving multiple suspects, it should include as many copies of Page One of the Suspicious Activity Report as there are suspects and complete a separate Part II

---

[28] FinCEN's Regulatory Helpline, (800) 949-2732, is the primary means for the financial community to obtain regulatory guidance and answers to specific questions.

[29] The Suspicious Activity Report Form completion tips in this section apply to forms filed electronically as well. For more information about FinCEN's BSA Direct E-Filing system, please visit the public website at http://bsaefiling.fincen.treas.gov.

for each suspect. The narrative should include a complete description of the transactions involved (time, place, type of transaction, type of instruments, amounts involved, circumstances that make the transactions suspicious, etc.) and a description of the relationship between or involvement of the suspects. For more information about completing an accurate narrative, see FinCEN's previous *Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative*, available at http://www.fincen.gov/sarnarrcompletguidfinal_112003.pdf.

2. Victims of Suspicious Activity

Another frequently asked question involves the completion of a Suspicious Activity Report if a financial institution discovers suspicious activity when one of its customers becomes a victim of a crime. For example, a customer may attempt to cash a fraudulent cashier's check that was provided to him or her to pay for goods the bank's customer sold. When the customer of a financial institution is the victim of a crime, the financial institution should not provide "Suspect Information" about the customer in Part II of the Suspicious Activity Report. The suspect that should be listed in Part II is the person, if known, who defrauded the bank's customer through the transaction involving the financial institution (in the example provided, the person who gave the customer the fraudulent cashier's check). The financial institution may include information about its customer/victim in the narrative portion of the Suspicious Activity Report.

3. Suspect Information Unavailable

A third question frequently received on the helpline concerns form completion when the financial institution does not have information about the suspect. Particularly for money services businesses, it is frequently the case that the financial institution has little or no identifying information about the suspect beyond a physical description. If suspect information is unknown or unavailable, the financial institution should mark the box in Part II of the Suspicious Activity Report form entitled "Suspect Information Unavailable." However, any partial or incomplete identifying information should be included in Part II, or in the narrative. For example, a customer/victim who attempts to cash a counterfeit check received as payment for goods, may be able to provide a description of the suspect, a name, or a phone number or an email address that was used to correspond with the suspect before the transaction.

Alternatively, a suspect may attempt a transaction, such as a funds transfer, but when asked for identification may terminate the transaction without providing any identification in a manner that raises suspicion. In those cases, the financial institution should include whatever identifying information is available in Part II (the name and/or phone number in the first example), and all other available information (email address, description, etc.) in the narrative. Responses commonly used to clarify why data is not being provided include: none, not applicable and unknown.[30]

4. Correcting vs. Updating a Prior Report

In Issue 6 of *The SAR Activity Review,*[31] FinCEN published guidance for "Filing a Corrected SAR Form." Although this article distinguished between the correcting of a Suspicious Activity Report, and what is commonly called the "90-day update" of a previously filed Suspicious Activity Report, FinCEN continues to receive inquiries about these requirements.

Corrected Report: When correcting an error on a previously filed report, mark box 1 ("corrects prior report") and follow the directions to make the necessary changes. Whenever a corrected report is filed, the institution should explain the changes in the Suspicious Activity Report narrative. For example:

- A financial institution would correct a prior report if it discovers a clerical error, such as an incorrectly reported name or address; or

- As part of its customary internal audit, a financial institution may find previously undetected suspicious activity related to a previously filed Suspicious Activity Report that had already been filed, in which case the date range, dollar amounts, summary characterization and narrative of the original Suspicious Activity Report may need to be amended.

---

[30] See Issue 6 of *The SAR Activity Review*- Trends, Tips & Issues, November 2003, page 51, at http://www.fincen.gov/sarreviewissue6.pdf

[31] See Issue 6 of *The SAR Activity Review*- Trends, Tips & Issues, November 2003, page 56, at http://www.fincen.gov/sarreviewissue6.pdf.

Updated Report: Correcting a prior report should not be confused with updating a Suspicious Activity Report for continued suspicious activity. Previous guidance specified that "as a general rule of thumb, organizations should report continuing suspicious activity with a report being filed at least every 90 days" (*The SAR Activity Review*, Issue 1 (October 2000, page 27). Unlike correcting an error on a previously filed Suspicious Activity Report, an update provides a detailed account of suspicious activity that has occurred since the last Suspicious Activity Report filing. For example:

- A large currency transaction log reveals that a customer is making cash withdrawals of just under $10,000 twice a week. After investigation, the financial institution concludes that there is no business or apparent lawful purpose for the transactions, and files a Suspicious Activity Report for structuring deposits to avoid reporting requirements. The customer continues the pattern of taking similarly structured withdrawals. Assuming the nature of the activity remains consistent, a new Suspicious Activity Report should be filed at 90-day intervals to update the last filed Suspicious Activity Report.

Technically, FinCEN's suspicious activity reporting rules require a Suspicious Activity Report for each suspicious transaction. However, for ongoing suspicious activity, and to reduce the burden on financial institutions and law enforcement,[32] FinCEN provided the above guidance to allow for updates every 90 days. FinCEN welcomes discussion of this guidance and will continue to consider the issue within the context of current regulations.

When filing a "90-day update," financial institutions should not check box 1, since an update does not actually correct a prior report. Instead, the financial institution should complete most of the Suspicious Activity Report as if it were the first report filed on the suspect's activity. The date range and dollar amounts should be cumulative, encompassing the entire period of suspicious activity (not just the last 90 days). The narrative does not need to detail the entire episode; rather, the narrative needs to only reference the previously filed Suspicious Activity Report(s), summarize the information previously reported, and then detail any activity that has occurred since the last report was filed (the previous 90 days of activity).

For situations where the nature of the activity reported changes after the original Suspicious Activity Report filing, the suspicious activity is no longer

[32] For more information, see *The SAR Activity Review- Trends, Tips & Issues*, Issue 1, page 27, at http://www.fincen.gov/sarreviewforweb.pdf.

considered “ongoing”--e.g., the customer in the above example begins sending or receiving funds in addition to making structured withdrawals. In such cases, the institution should consider the changed activity a new transaction and should file a new Suspicious Activity Report within the normal filing deadlines, rather than updating a previous filing after 90 days. Because the activity is related, however, it may be appropriate to cross-reference any previously filed Suspicious Activity Reports in the narrative. Further, if previously reported activity ceases, no further Suspicious Activity Reports need to be filed.

Section 5 – Issues & Guidance

This section of *The SAR Activity Review* discusses current issues raised with regard to the preparation and filing of Suspicious Activity Reports. This section is intended to identify suspicious activity reporting-related issues and provide meaningful guidance to filers; in addition, it reflects the collective positions of the government agencies that require organizations to file Suspicious Activity Reports. **Note:** This guidance will also be separately posted to FinCEN's public website at www.fincen.gov**.**

National Security Letters and Suspicious Activity Reporting

National Security Letters are written investigative demands, somewhat analogous to administrative subpoenas that can be issued by the Federal Bureau of Investigation in counterintelligence and counterterrorism investigations to obtain the following:

- telephone and electronic communications records from telephone companies and Internet Service Providers (pursuant to the Electronic Communications Privacy Act, 18 USC 2709);
- information from credit bureaus (pursuant to the Fair Credit Reporting Act, 15 USC 1681u); and
- financial records[33] from financial institutions[34] (pursuant to the Right to Financial Privacy Act of 1978, 12 USC 3401 *et seq*.).[35]

---

[33] Under the Right to Financial Privacy Act of 1978 ("RFPA"), "financial records" are defined as "an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution." 12 USC 3401(2).

[34] Section 374 of the Intelligence Authorization Act for Fiscal Year 2004 (Pub. Law 108-177 (Dec. 13, 2003) amended the definition of "financial institution" for purposes of the Right to Financial Privacy Act of 1978 (12 USC 3414) to incorporate the definition of "financial institution" in the Bank Secrecy Act, 31 USC 5312(a)(2) and (c)(1).

[35] The USA PATRIOT Act changed the standard predicate for FBI RFPA National Security Letters to one requiring that the information being sought through the National Security Letter is "for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States." The USA PATRIOT Act also provided authority for the Director of the FBI to delegate signature authority for National Security Letters to Special Agents in Charge serving in designated field divisions.

National Security Letters can also be issued by other federal government authorities for purposes of conducting foreign counter or positive-intelligence activities,[36] certain protective functions,[37] or intelligence or counter intelligence analyses related to international terrorism[38] to obtain financial records from financial institutions.[39]

National Security Letters are highly confidential investigative tools employed by the federal government. Financial institutions that receive National Security Letters must take appropriate measures to ensure the confidentiality of the letters. FinCEN encourages financial institutions to have procedures in place for processing and maintaining the confidentiality of National Security Letters.[40]

Mere receipt of a National Security Letter does not, by itself, require the filing of a Suspicious Activity Report by the financial institution receiving the letter. Nonetheless, the National Security Letter is a piece of information that may be relevant to a financial institution's overall risk assessment of its customers and accounts. It is incumbent upon a financial institution to assess the information in accordance with its risk-based anti-money laundering program, policies and procedures, and to determine whether a Suspicious Activity Report should be filed based on the totality of information available to the institution. In any event, all regulatory suspicious activity triggers and dollar thresholds for filing Suspicious Activity Reports would apply. So, for instance, under FinCEN's suspicious activity reporting requirements at 31 CFR 103.18, banks are required to file a Suspicious Activity Report for transactions conducted or attempted by, at, or through the bank involving or aggregating at least $5,000, and the bank knows, suspects, or has reason to suspect that (1) the transaction involves funds derived from illegal activity or

---

[36] Foreign counter- or positive-intelligence activities could include, for example, the audit of customer records of a financial institution related to the clandestine activities of an intelligence agency, pursuant to the RFPA, 12 U.S.C. §314(a)(1)(A). *See, e.g., Duncan v. Belcher*, 813 F.2d 1335, 1339 and 1339 n. 1 (4th Cir. 1987).

[37] The RFPA, 12 U.S.C. §3414(a)(1)(B), permits certain disclosures of financial records to the United States Secret Service for the purposes of conducting its protective functions.

[38] The RFPA, 12 U.S.C. § 3414(a)(1)(C), permits certain disclosure of financial records pursuant to a request from a federal government agency authorized to conduct investigations or intelligence or counterintelligence analyses related to international terrorism.

[39] In Doe v. Ashcroft, 334 F. Supp.2d 471 (S.D.N.Y. 2004), a federal district court held that 18 U.S.C. 2709, which authorizes the issuance of national security letters to Internet service providers, is unconstitutional on account of its nondisclosure provisions and lack of judicial review. The Federal Bureau of Investigation appealed the decision and obtained a stay pending appeal, so it is continuing to issue national security letters under that statute. That decision did not adjudicate the constitutionality of the statute authorizing the issuance of national security letters to financial institutions, 12 U.S.C. 3414.

[40] Pursuant to 12 U.S.C. § 3414(a)(3) and (5)(D), no financial institution, or officer, employee or agent of the institution, can disclose to any person that a government authority or the FBI has sought or obtained access to records through an RFPA National Security Letter.

is intended or conducted in order to hide or disguise funds or assets derived from illegal activities; (2) the transaction is designed to evade any requirements under the Bank Secrecy Act; or (3) the transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts.[41]

If a financial institution does file a Suspicious Activity Report relating to information in a National Security Letter, no reference to the receipt or existence of the National Security Letter should be made in any part of the Suspicious Activity Report, including the narrative. Instead, the Suspicious Activity Report should reference only facts and activities underlying or derived from the information in the National Security Letter; only those facts and activities should be detailed in the report.

Because the range of financial institutions that may receive National Security Letters comprises all financial institutions referenced in the Bank Secrecy Act, and because there are a number of federal regulatory agencies responsible for examining and supervising many of these financial institutions, FinCEN is working with the other federal financial institution regulators to develop consistent policies on these issues on an interagency basis.[42]

If a financial institution has questions about Suspicious Activity Report filing relating to National Security Letters, or about Suspicious Activity Reporting in general, it should contact FinCEN's Regulatory Helpline at (800) 949-2732. Financial institutions having a federal functional regulator may also wish to contact their federal functional regulator for questions relating to that regulator's suspicious activity reporting requirements and to procedures and records that the institution should maintain. Questions regarding National Security Letters should be directed to the financial institution's local Federal Bureau of Investigation field office. Contact information for Federal Bureau of Investigation field offices can be obtained from the FBI's website at www.fbi.gov.

---

[41] Each Federal bank regulatory agency has adopted suspicious activity reporting requirements that contain additional factors and triggers, including (1) involvement of an insider (no dollar threshold); (2) over $5,000 is involved and the institution can identify a suspect; (3) over $25,000 is involved but the institution cannot identify a suspect; or (4) the transaction involves $5,000 or more and involves potential money laundering or violations of the Bank Secrecy Act. *See, e.q.,* 12 CFR 21.11(c). Furthermore, under FinCEN's suspicious activity reporting requirements, the dollar thresholds vary (*e.g.,* for casinos and broker-dealers in securities, the dollar threshold is at least $5,000; for money services businesses, the dollar threshold is at least $2,000 or $5,000 if the identification of transactions is derived from a review of clearance records.)

[42] See Office of the Comptroller of the Currency Interpretive Letter #1003, "Suspicious Activity Reports" (Aug. 2004).

Revised Guidance on Filing Suspicious Activity Reports Relating to the Office of Foreign Assets Control *List of Specially Designated Nationals and Blocked Persons*

In an effort to eliminate duplicative reporting, on December 23, 2004, FinCEN published a final rule updating previous guidance on filing Suspicious Activity Reports involving individuals or entities designated by the Department of Treasury's Office of Foreign Assets Control (OFAC) as a threat to United States policy or national security.[43] As a way of enforcing economic and trade sanctions, the Office of Foreign Assets Control requires a United States financial institution to block transactions involving people or organizations that are specially designated.[44] The revised guidance generally clarifies that blocking reports filed with the Office of Foreign Assets Control will be deemed by FinCEN to satisfy the requirement to file Suspicious Activity Reports on such transactions.

Previous Guidance

The Bank Secrecy Act and FinCEN's implementing rules require banks, securities broker-dealers, introducing brokers, casinos, futures commission merchants, and money services businesses to report suspicious activity that meets a particular threshold, which differs depending on the entity. Generally, the rules provide a financial institution with thirty days from the date of the initial detection of suspicious activity to file a Suspicious Activity Report, with an additional thirty days if the financial institution is unable to identify a suspect. Reports are filed on forms developed for each industry subject to the reporting requirement.

The Office of Foreign Assets Control requires any person, including a United States financial institution, to file reports regarding blocked financial accounts, payments or transfers in which an Office of Foreign Assets Control

---

[43] See Interpretive Release Number 2004-02-Unitary Filing of Suspicious Activity and Blocking Reports, 67 FR 76847 (December 23, 2004).

[44] The designations are as follows: specially designated terrorist; foreign terrorist organization; specially designated global terrorist; specially designated narcotics trafficker; specially designated narcotics trafficker kingpin. A blocked transaction relates to an account to which payments, transfers, withdrawals, or other dealings may not be made except as licensed by the Office of Foreign Assets Control or otherwise authorized by the Treasury Department. See 31 CFR parts 595, 597, 598 and the Foreign Narcotics Kingpin Act, 21 USC 1901-08, 8 USC 1182. These categories of designations are subject solely to blocking requirements.

designated country, entity or individual has any interest.[45] Reports must be filed with the Office of Foreign Assets Control within ten business days of the blocking of the property. Transactions involving an individual or entity designated on the Office of Foreign Assets Control *List of Specially Designated Nationals and Blocked Persons* as a global terrorist, terrorist, terrorist organization, narcotics trafficker, or narcotics kingpin may be in furtherance of a criminal act, and therefore relevant to a possible violation of law. Thus, blocking reports related to such persons also describe potentially suspicious activity.

FinCEN was receiving numerous questions about whether a financial institution was required to file a Suspicious Activity Report with FinCEN when it had a verified match on persons or entities on one of the Office of Foreign Assets Control lists. In Issue 6 of *The SAR Activity Review* (November 2003), FinCEN provided the following guidance on the issue:

> *A verified match with an entity on an OFAC list that involves funds in an amount above the applicable SAR filing threshold should trigger a SAR filing requirement.*[46]

While this guidance ensured that the relevant information would be available to law enforcement, it also resulted in financial institutions being required to make two separate filings with the Department of the Treasury - one with the Office of Foreign Assets Control pursuant to its Reporting, Procedures and Penalties Regulations, and one with FinCEN pursuant to its Suspicious Activity Reporting rules.

Revised Guidance

Upon further consideration, FinCEN revised its prior guidance to allow a financial institution to satisfy its obligation to file a Suspicious Activity Report on a transaction involving a person designated as a Specially Designated Global Terrorist, a Specially Designated Terrorist, a Foreign Terrorist Organization, a Specially Designated Narcotics Trafficker Kingpin, or a Specially Designated Narcotics Trafficker by filing a blocking report with the Office of Foreign Assets Control. This guidance does not affect a

[45] See 31 CFR 501.603.
[46] See page 64 at http://www.fincen.gov/sarreviewissue6.pdf.

financial institution's obligation to identify and report suspicious activity beyond the fact of the Office of Foreign Assets Control match. To the extent that the financial institution is in possession of information not included on the blocking report filed with the Office of Foreign Assets Control, a separate Suspicious Activity Report should be filed with FinCEN including that information. This guidance also does not affect a financial institution's obligation to file a Suspicious Activity Report even if it has filed a blocking report with the Office of Foreign Assets Control, to the extent that the facts and circumstances surrounding the Office of Foreign Assets Control match are independently suspicious and are otherwise required to be reported under the existing FinCEN regulations. In those cases, the Office of Foreign Assets Control blocking report would not satisfy a financial institution's Suspicious Activity Report filing obligation.

The Office of Foreign Assets Control will provide FinCEN the information in the blocking reports for inclusion in the Suspicious Activity Report database. Accordingly, the revised guidance serves two useful purposes: (1) allows for expedited information to law enforcement and (2) reduces the suspicious-activity-reporting burden on the industry.

Since the issuance of the guidance, FinCEN has been asked about the filing of Suspicious Activity Reports for transactions subject to reject reports[47] filed with the Office of Foreign Assets Control. When a financial institution files a reject report on a transaction, the financial institution is obligated to file a Suspicious Activity report to the extent that the facts and circumstances surrounding the rejected funds transfer are suspicious. For example, a financial institution need not file a Suspicious Activity report on a rejected funds transfer involving Iraq unless the facts surrounding the transaction are themselves suspicious.

---

[47] Reject reports are required to be filed with OFAC by financial institutions that reject a funds transfer where the funds are not blocked under OFAC rules but where processing the transfer would nonetheless violate, or facilitate an underlying transaction that is prohibited under OFAC rules. See 31 CFR 501.604. Examples of transactions involving rejected funds transfers include funds transfer instructions referencing a blocked vessel but where none of the parties of financial institutions involved in the transactions is a blocked person, as well as transactions with Iraq, Iran, or the Governments of Iran, Syria or Sudan.

Suspicious Activity Involving the Iraqi Dinar

Over the last year, the circumstances of the war in Iraq have created the phenomenon of businesses trading in new Iraqi dinars. Many of these businesses advertise or conduct business over the Internet, and suggest that the Iraqi dinar, much like the Kuwaiti dinar following Operation Desert Storm, will increase in value exponentially following United States military involvement in Iraq. Most investors purchase dinars from websites established particularly for selling dinars or from major auction websites.

FinCEN has been receiving inquiries regarding the legitimacy of websites offering Iraqi dinar sales. While it is not necessarily illegal to buy or sell Iraqi currency, there are a number of risks and compliance concerns for the financial community. For example, Iraqi officials state that it is illegal under Iraqi law to export dinars. Therefore, in addition to questions about the source of the currency, and the potential for investment or securities fraud, businesses offering to sell dinars may also pose the risk of being used to fund terrorism or as a vehicle for money laundering. FinCEN also has a particular interest in these businesses because they may be money services businesses required to comply with the Bank Secrecy Act.

Any United States entity that buys or sells currency, including Iraqi dinars, in amounts of more than $1,000 U.S. to any one person in one day may be a money services business under FinCEN's regulations at 31 C.F.R. Section 103.11(uu). [Note: there have been questions about the old dinar with Hussein's picture on it. That dinar ceased to be legal tender around January 15, 2004 and thus ceased to be currency for purposes of the Bank Secrecy Act.] Money services businesses include:

- Money transmitters;
- Currency Dealers or Exchangers (except those who do not exchange more than $1,000 in currency or monetary or other instruments for any person on any day in one or more transactions);
- Check cashers (except those who do not cash checks in an amount greater than $1,000 in currency or monetary or other instruments for any person on any day in one or more transactions);
- Issuers, sellers, or redeemers of traveler's checks, money orders, or stored value (except those who do not issue, sell or redeem such instruments in an amount greater than $1,000 in currency or monetary or other instruments for or from any person on any day in one or more transactions);

Money services businesses generally are required to register with FinCEN, to establish anti-money laundering programs, and to comply with recordkeeping and reporting requirements under the Bank Secrecy Act. Dinar sales websites frequently claim that their businesses are registered with the Department of the Treasury. These assertions are not always accurate. Further, it may be difficult to discern from the money services business registration list on FinCEN's website (www.msb.gov) whether the business is in fact registered, particularly if the business is an affiliate of, or a "doing business as" alias for, the business that is registered. Moreover, even if the business is registered with FinCEN, that registration does not guarantee that the business is in compliance with other Bank Secrecy Act requirements or with applicable state law. For these reasons, a financial institution that conducts business with entities selling Iraqi dinars should conduct appropriate due diligence to assure itself of the legitimacy of such entities. All financial institutions that do business with, and potential customers of, such money services businesses, are reminded that registration with FinCEN in no way authenticates either the legitimacy of a business, or the compliance of the business with any federal, state, or local laws.

An analysis of FinCEN's Suspicious Activity Report database for filings referencing Iraqi dinars indicated suspicion of the use of Internet dealers of Iraqi dinars in terrorist financing, although not all of the corresponding narratives provided clear or complete justification about the terrorist financing nature of the activity reported. This serves as a potent illustration of the critical importance of a clear and complete narrative description when filing a Suspicious Activity Report. Particularly when terrorist financing is suspected, conclusory statements with no supporting facts or justification are of limited use to law enforcement in pursuing their investigations.

Further analysis of businesses engaged in dinar sales is ongoing. For instance, FinCEN analyzed Bank Secrecy Act data (including Suspicious Activity Reports, Currency Transaction Reports, and Reports of International Transportation of Currency or Monetary Instruments) involving the purchase of Iraqi dinars to support a law enforcement initiative that uncovered an elaborate network of structured money movement by and to persons suspected or convicted of substantial fraud or other illicit international activities.

Section 6 – Industry Forum

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

An Overview of Suspicious Activity Report Training Elements in 2005

By John Byrne, representing the American Bankers Association, and Robert Rowe, representing the Independent Community Bankers of America (ICBA), to the Bank Secrecy Act Advisory Group

It is certainly appropriate to discuss key elements of a Suspicious Activity Report (SAR) training program in *The SAR Activity Review***.** Clearly, *The Review* includes useful resources that financial institutions can use to provide employees with information needed to enhance and improve their Suspicious Activity Report (SAR) procedures. These resources are needed because, as we have all witnessed, the spate of recent enforcement orders often contain language such as:

Within 60 days of this Agreement, the Bank shall submit to the [agency] an acceptable written plan to provide effective training to all appropriate personnel at the [location] in all aspects of regulatory and internal policies and procedures related to the Bank Secrecy Act (BSA) and the ***identification and reporting of suspicious transactions****, and to* ***update*** *the training on a regular basis to reasonably ensure that all personnel are trained in the most current legal requirements and in the organization's risk management processes.*

In addition, the Office of the Comptroller of the Currency (OCC) has indicated in their "enforcement guidance for BSA/AML program deficiencies" that a cease and desist order (C&D) will be issued if, among other things, the bank lacks a BSA (Bank Secrecy Act) compliance program that covers elements such as training. (See OCC 2004-50, issued November 10, 2004).

How can banks be sure they have the proper resources to handle Suspicious Activity Report training? This question is beyond the scope of this section but we can point you in the right direction.

Training Parameters

In order to prepare your employees to handle situations that demand Suspicious Activity Report consideration and the possible filing of a Suspicious Activity Report, an institution must first outline for its employees the Suspicious Activity Report related categories of suspicious activities on the Suspicious Activity Report filing form. Banks are not expected to be experts in the nuances of each listed crime on the form but a general description of what is clearly reportable is necessary. From mortgage loan fraud to false statements, the list of crimes is defined in the last edition of the *SAR Activity Review*. However, appropriate employees should be familiar with the types of suspicious activities covered by the Suspicious Activity Report form and the elements of those activities so that they know what to look for.

Training staff on the categories of Suspicious Activity Report (SAR)-related crimes also will help address the confusion that exists beyond the compliance function that Suspicious Activity Reports must be filed simply if there is "suspicious activity." As we know, Suspicious Activity Reports should be filed after careful analysis of the facts of a given transaction or series of transactions and not by impulse. Explaining the various Suspicious Activity Report categories and what potentially makes an activity suspicious may assist in alleviating this confusion.

Once the institution creates the basic elements of a Suspicious Activity Report training program, the decision must be reached on who must be trained and what level of training is needed. Since all employees must be aware of the Suspicious Activity Report program, training must be across-the-board. Training for those not involved in the day-to-day aspects of security or compliance can be broad and should at least contain a general description of the suspicious activities listed on the Suspicious Activity Report form. For employees with greater responsibility for the bank's Anti-Money Laundering (AML) compliance program, especially those who make the final decision that a Suspicious Activity Report should be filed, training should be more comprehensive. A variety of sources are available to assist banks with this training, whether it is done in-house or through a trusted third party provider. For example, a bank might choose to rely on audio-conferences, one-day seminars, video training or other materials to properly train employees. However, it is important that the bank develop a training program for its employees.

An institution can supplement this type of training by information through in-house newsletters, encouraging staff to sign up for government agency on-line updates and other outside sources. Whatever the source, it is critical that this broad training be updated frequently with mention of major news stories or enforcement actions. Since suspicious activities are constantly evolving, it is important that appropriate bank employees have access to information about current developments in suspicious activities.

For those involved in Anti-Money Laundering (AML) and Bank Secrecy Act (BSA) oversight in the institution, it is recommended that the staff attend compliance schools, achieve professional certification, and participate in national and regional Anti-Money Laundering (AML) programs on an annual basis. As mentioned above, the increased availability of on-line or remote Bank Secrecy Act/Suspicious Activity Report (BSA/SAR) training makes it easier to stay current with Suspicious Activity Report issues and other reporting mandates.

Suspicious Activity Report Related Resources

Some of us on the Bank Secrecy Act Advisory Group (BSAAG) remember a time when available resources were in hard bound binders that were updated annually. Now, compliance officers can get access to training materials or supplements with the click of a mouse and without cost. Take advantage of the myriad of government resources as you prepare your Suspicious Activity Report (SAR) training materials. We recommend:[48]

- FinCEN's website
- *The SAR Activity Review*, including all back issues;
- Information from your Anti-Money Laundering (AML) software vendor;
- Anti-Money Laundering (AML) seminars
- Compliance publications;
- Federal banking agency websites;
- Federal law enforcement sites such as the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI) and others;
- Your friendly neighborhood national or state trade association

As you struggle with compliance in this new environment, it is comforting to know that critical information is available to assist you in this challenge.

---

[48] Neither the Bank Secrecy Act Advisory Group (BSAAG) nor any government agency may recommend any commercial software vendor or any non-governmental seminar sponsor.

Section 7 - Feedback Form

Financial Crimes Enforcement Network
Department of the Treasury

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

A. Please identify your type of financial institution.

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

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

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

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

Other (please identify): _____

B. Please indicate your level of satisfaction with each section of this issue of *The SAR Activity Review- Trends Tips and Issues* (circle your response).
1=Not Useful, 5=Very Useful

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

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

_____
_____
_____
_____

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

_____

_____

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

Yes No

F. Did you review and/or use the December 2004 issue of *The SAR Activity Review – By the Numbers*?

Yes No

If yes, how do you use the statistical data in *By the Numbers*?

_____

_____

What other statistical data would you find interesting or useful?

_____

_____

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

_____

_____

_____

_____

H. What topics would you like to see in the next or future editions of the *The SAR Activity Review – Trends, Tips and Issues*? Please be specific, i.e., ATM activity conducted through independently owned ATMS, rather than just ATM activity.

_____

_____

_____

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

_____

_____

_____

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

[ ] October 2000 [ ] June 2001 [ ] October 2001 [ ] August 2002
[ ] February 2003 [ ] November 2003 [ ] August 2004

Fax Feedback Forms to:

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

Appendix

Index of Topics from previous issues of The SAR Activity Review

Topic	Issue	Page	Hyperlink Address to *SAR Activity Review* Issue
Automated Teller Machine (ATM) Commonly Filed Violations	7	23	http://www.fincen.gov/sarreviewissue7.pdf
Automobile Retail Industry: SAR Analysis – Indications of Suspicious Activity	5	27	http://www.fincen.gov/sarreviewissue5.pdf
Boat/Yacht Retail Industry: SAR Analysis – Indications of Suspicious Activity	5	31	http://www.fincen.gov/sarreviewissue5.pdf
Broker-Dealer SARs – The First Year	7	20	http://www.fincen.gov/sarreviewissue7.pdf
Casino and Card Club Industries – Suspicious Activity Report Filings	8	19	http://www.fincen.gov/sarreviewissue8.pdf
Computer Intrusion	3	15	http://www.fincen.gov/sarreviewissue3.pdf
Consumer Loan Fraud	7	27	http://www.fincen.gov/sarreviewissue7.pdf
Correspondent Accounts and Shell Company Activity	2	18	http://www.fincen.gov/sarreview2issue4web.pdf
Coupon Redemption Fraud	6	14	http://www.fincen.gov/sarreviewissue6.pdf
Credit/Debit Cards: Suspicious Activity	4	29	http://www.fincen.gov/sarreview082002.pdf
Director's Forum: Issue 8	8	3	http://www.fincen.gov/sarreviewissue8.pdf
Egmont Group- Strategic Analysis Initiative	2	24	http://www.fincen.gov/sarreview2issue4web.pdf
FATF Typologies Exercise	2	23	http://www.fincen.gov/sarreview2issue4web.pdf
Food Stamp Fraud Using Electronic Benefit Transfer (EBT) Cards	7	9	http://www.fincen.gov/sarreviewissue7.pdf
Global Use of SARs	2	24	http://www.fincen.gov/sarreview2issue4web.pdf
Index of Topics from Previous SAR Activity Review Issues	6	85	http://www.fincen.gov/sarreviewissue6.pdf
Identity Theft	2	14	http://www.fincen.gov/sarreview2issue4web.pdf
Identity Theft – Update	3	24	http://www.fincen.gov/sarreviewissue3.pdf
Increased SAR Reporting Involving Mexico	1	12	http://www.fincen.gov/sarreviewforweb.pdf
Indicators of Misuse of Informal Value Transfer Systems	5	18	http://www.fincen.gov/sarreviewissue5.pdf
Industry Forum: Check Fraud Loss Report	5	69	http://www.fincen.gov/sarreviewissue5.pdf
Industry Forum: Check Fraud Loss Report	1	29	http://www.fincen.gov/sarreviewforweb.pdf
Industry Forum: FinCEN & Regulatory Agencies Respond to Industry Forum Comments	7	51	http://www.fincen.gov/sarreviewissue7.pdf
Industry Forum: Number of SAR Filings Should Not Determine Adequate SAR Program	7	49	http://www.fincen.gov/sarreviewissue7.pdf
Industry Forum: Questions and Answers on MSBs	2	38	http://www.fincen.gov/sarreview2issue4web.pdf
Industry Forum: Some Tips for Auditing the Suspicious Activity Reporting Program	6	71	http://www.fincen.gov/sarreviewissue6.pdf
Industry Forum: Recommended Security Procedures for Protecting Customer Information	3	45	http://www.fincen.gov/sarreviewissue3.pdf
Industry Forum: Safe Harbor Protection for Employment References	4	53	http://www.fincen.gov/sarreview082002.pdf
Industry Forum: An Overview of Suspicious Activity Report Training Elements in 2005	8	43	http://www.fincen.gov/sarreviewissue8.pdf
Issues and Guidance: Advanced Fee Schemes	4	49	http://www.fincen.gov/sarreview082002.pdf

Issues and Guidance: Applicability of Safe Harbor	3	44	http://www.fincen.gov/sarreviewissue3.pdf
Issues and Guidance: Applicability of Safe Harbor	2	37	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: BSA Guidance – IRS Computing Center / FinCEN Help Line & Website	6	65	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Cessation of Relationship/Closure of Account	1	27	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: Disclosure of SAR Documentation	2	36	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Disclosure of SARs and Underlying Suspicious Activity	1	28	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: FAQs from FinCEN Help Line – 314a Process	6	59	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: FAQs from FinCEN Help Line – MSB SAR Reporting Questions	6	61	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Filing SARs on Activity Outside the United States	2	35	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Filing SARs on Continuing Activity after Law Enforcement Contact	2	35	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Filing SARs on OFAC List or 314(a) Matches	6	64	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Financial Institutions Hotline	3	43	http://www.fincen.gov/sarreviewissue3.pdf
Issues and Guidance: Florida Appeal Court Decision re: SAR production	6	65	http://www.fincen.gov/sarreviewissue6.pdf
Issues and Guidance: Guidance as to What to do When Asked for Production of SARs	7	45	http://www.fincen.gov/sarreviewissue7.pdf
Issues and Guidance: National Security Letters and Suspicious Activity Reporting	8	35	http://www.fincen.gov/sarreviewissue8.pdf
Issues and Guidance: Office of Foreign Assets Control (OFAC)	4	49	http://www.fincen.gov/sarreview082002.pdf
Issues and Guidance: Office of Foreign Assets Control's List of Specially Designated Nationals and Blocked Persons- Revised Guidance on filing Suspicious Activity Reports	8	38	http://www.fincen.gov/sarreviewissue8.pdf
Issues and Guidance: PATRIOT Act Communications System	5	65	http://www.fincen.gov/sarreviewissue5.pdf
Issues and Guidance: Prohibition on Notification	2	36	http://www.fincen.gov/sarreview2issue4web.pdf
Issues and Guidance: Repeated SAR Filings on Same Activity	1	27	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: SAR Disclosure as part of Civil Litigation	4	50	http://www.fincen.gov/sarreview082002.pdf
Issues and Guidance: SAR Guidelines for Reporting Advance Fee Schemes	7	47	http://www.fincen.gov/sarreviewissue7.pdf
Issues and Guidance: SAR Rulings: SAR Disclosure	5	66	http://www.fincen.gov/sarreviewissue5.pdf
Issues and Guidance: Suspicious Activity Involving the Iraqi Dinar	8	41	http://www.fincen.gov/sarreviewissue8.pdf
Issues and Guidance: Timing for SAR filings	1	27	http://www.fincen.gov/sarreviewforweb.pdf
Issues and Guidance: USA PATRIOT Act: 314(a) Information Requests	5	66	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: 314(a) Results Enhance Material Support for Terrorism Case	7	30	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Attorney and Three Accomplices Convicted in Multi-Million Dollar Real Estate Fraud	7	35	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Black Market Peso Exchange	2	28	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Bank President Guilty in Loan Fraud	7	34	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Bankruptcy Bust-out Scheme	6	42	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Bankruptcy Fraud Involving Family Members	6	41	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: BSA Data Leads to $18 Million Seizure	7	31	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Charity Evades Reporting Requirement	8	26	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Check Cashing Business	3	34	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Check Kiting Suspect	2	29	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Cocaine Trafficker	2	30	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Computer Chip Theft Ring	3	33	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Conviction of Pharmacist	5	54	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Counterfeit Check Fraud	1	17	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Credit Card Theft	2	30	http://www.fincen.gov/sarreview2issue4web.pdf

Law Enforcement Case: Criminal Organization – Baby Formula	1	18	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Customs Fraud	1	17	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Drug Money Laundering	1	22	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Drug Trafficker Forfeits Structured Cash	7	35	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Drug Trafficking and Money Laundering	2	29	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Embargo Investigation	2	28	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Embezzlement	1	16	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Extortion and Title 31	3	29	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Food Bank Theft	1	19	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Forgery of U.S. Treasury Checks	6	44	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Former Banker Sentenced for Avoiding IRS Reporting	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Hawala Investigation	6	38	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Hawala Operation	8	26	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Illegal Casa de Cambio	3	34	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Illegal Money Transfers to Iran	5	51	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Illegal Money Transfers to Iraq	4	35	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Importance of SAR Reporting to Law Enforcement Investigations	3	37	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Individual Operating as Unlicensed Money Transmitter	7	30	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Insider Fraud Contributes to Bank Failure	8	28	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Insurance Executive Embezzled from Local Government's Self-Insured Health Fund	7	36	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Internal Fraud at Local Bank	5	54	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: International Money Laundering Case	4	36	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Investment Firm CEO	5	53	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Investment Fraud Scheme	6	43	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Investment Fraud Scheme	1	16	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Investment Scam	3	30	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Marijuana Farm Owner Sentenced	8	27	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Medicaid Fraud	1	22	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Metal Traders Charged in International Bank Fraud Scheme	4	36	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Methamphetamine Production Ring	3	31	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Money Laundering and Pyramid Scheme	8	28	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Money Laundering by RV Dealer	3	30	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Money Laundering in Maryland	4	39	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Money Laundering involving Insurance Industry	5	53	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Money Laundering involving Iraq	6	39	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Money Laundering of Marijuana Sales Proceeds	6	44	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Money Remitter Sending Money to Iraq	5	52	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Money Remitting Business Laundering Drug Proceeds	8	28	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Nigerian Advance Fee Scam	6	40	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Nigerian Round-Tripping Investigation	7	32	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Non-Profit Organization Operating as Money Remitter	7	31	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Operation Mule Train	1	18	http://www.fincen.gov/sarreviewforweb.pdf

Law Enforcement Case: Organized Crime Network	1	18	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Phantom Bank Scheme	2	30	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Ponzi Scheme	2	26	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Ponzi Scheme	7	31	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Securities Dealer	2	28	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Sports Betting Ring	3	31	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Sports Card Theft	3	32	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Stock Fraud	1	21	http://www.fincen.gov/sarreviewforweb.pdf
Law Enforcement Case: Stolen Check Ring	3	32	http://www.fincen.gov/sarreviewissue3.pdf
Law Enforcement Case: Stolen Check Scheme	2	31	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Structured Deposits Exceeding $700,000	7	34	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Structuring and Food Stamp Fraud	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Structuring by Three Family Members	4	37	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Tax Evasion Case	4	38	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Tax Evasion by a Business Owner	8	27	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Telemarketing Fraud	7	33	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Terrorism Investigation	8	25	http://www.fincen.gov/sarreviewissue8.pdf
Law Enforcement Case: Travel Agent	2	29	http://www.fincen.gov/sarreview2issue4web.pdf
Law Enforcement Case: Unlicensed Money Remitter ($1.2 million)	6	40	http://www.fincen.gov/sarreviewissue6.pdf
Law Enforcement Case: Unlicensed Money Remitter ($3 million)	5	52	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Unlicensed Money Remitter ($427,000)	5	51	http://www.fincen.gov/sarreviewissue5.pdf
Law Enforcement Case: Unlicensed Money Transmission Scheme	4	35	http://www.fincen.gov/sarreview082002.pdf
Law Enforcement Case: Unlicensed South American Money Exchanger	7	32	http://www.fincen.gov/sarreviewissue7.pdf
Law Enforcement Case: Worker's Compensation Fraud	1	20	http://www.fincen.gov/sarreviewforweb.pdf
Life Insurance: SAR Analysis – Indications of Suspicious Activity	5	35	http://www.fincen.gov/sarreviewissue5.pdf
Mailbag and Feedback	6	79	http://www.fincen.gov/sarreviewissue6.pdf
Mailbag & Feedback – Review of BSA/Structuring/Money Laundering Violation on SAR Forms	7	53	http://www.fincen.gov/sarreviewissue7.pdf
Mailbag – Questions from the Industry	3	49	http://www.fincen.gov/sarreviewissue3.pdf
Money Services Businesses: SARs filed by MSBs	4	33	http://www.fincen.gov/sarreview082002.pdf
Money Transmitter Activity	2	18	http://www.fincen.gov/sarreview2issue4web.pdf
Money Transmitters may be Money Laundering Vehicle	3	17	http://www.fincen.gov/sarreviewissue3.pdf
Multilateral Illicit Currency Flows Study	2	23	http://www.fincen.gov/sarreview2issue4web.pdf
Non-Cooperative Countries and Territories	3	27	http://www.fincen.gov/sarreviewissue3.pdf
Non-Cooperative Countries and Territories	2	22	http://www.fincen.gov/sarreview2issue4web.pdf
Non-Cooperative Countries and Territories	1	15	http://www.fincen.gov/sarreviewforweb.pdf
On-line and/or Internet Banking	6	27	http://www.fincen.gov/sarreviewissue6.pdf
Pawn Brokers: SAR Analysis – Indications of Suspicious Activity	5	33	http://www.fincen.gov/sarreviewissue5.pdf
Percentage of SARs Reporting Structuring	3	25	http://www.fincen.gov/sarreviewissue3.pdf
Pre-paid Telephone Cards	2	19	http://www.fincen.gov/sarreview2issue4web.pdf
Real Estate Industry – Sales and Management SARS	6	31	http://www.fincen.gov/sarreviewissue6.pdf
Refund Anticipation Loan (RAL) Fraud	7	15	http://www.fincen.gov/sarreviewissue7.pdf
Regional Money Remitter Activity	1	13	http://www.fincen.gov/sarreviewforweb.pdf
Reports of Solicitation Letters (Advanced Fee Fraud or 4-1-9 Scams)	3	23	http://www.fincen.gov/sarreviewissue3.pdf

Role of SARs in High Risk Money Laundering and Related Financial Crime Areas	1	14	http://www.fincen.gov/sarreviewforweb.pdf
Russian Criminal Activity	1	12	http://www.fincen.gov/sarreviewforweb.pdf
SAR News Update: Expansion of PACS	6	67	http://www.fincen.gov/sarreviewissue6.pdf
SAR News Update: Expansion of SAR and AML Compliance Requirements to New Industries	4	46	http://www.fincen.gov/sarreview082002.pdf
SAR News Update: Expansion of SAR Requirements to New Industries	5	61	http://www.fincen.gov/sarreviewissue5.pdf
SAR News Update: Financial Industries Required to File SARs	6	69	http://www.fincen.gov/sarreviewissue6.pdf
SAR News Update: FinCEN's Financial Institutions Hotline	4	45	http://www.fincen.gov/sarreview082002.pdf
SAR News Update: Non-Cooperative Countries and Territories	6	68	http://www.fincen.gov/sarreviewissue6.pdf
SAR News Update: Proposed Revision to Suspicious Activity Report	5	62	http://www.fincen.gov/sarreviewissue5.pdf
SAR News Update: USA PATRIOT Act: Section 311 Authority	5	62	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Computer Intrusion and Frequently Asked Questions	3	38	http://www.fincen.gov/sarreviewissue3.pdf
SAR Tips: Definitions and Criminal Statutes for SAR Characterizations of Suspicious Activity	7	39	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Filing a Corrected or Amended SAR	4	42	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: Filing a SAR for Ongoing or Supplemental Information	4	43	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: Frequently Asked Questions Received on FinCEN's Regulatory Helpline	8	29	http://www.fincen.gov/sarreviewissue8.pdf
SAR Tips: How do I . . .?	7	38	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Identity Theft and Pretext Calling	3	41	http://www.fincen.gov/sarreviewissue3.pdf
SAR Tips: Importance of Accurate and Complete Narratives	5	55	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Importance of the Narrative	2	32	http://www.fincen.gov/sarreview2issue4web.pdf
SAR Tips: Improvements to Eliminate Reporting Deficiencies	6	49	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: Informal Value Transfer System--Special SAR Form Completion Guidance	5	57	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Instructions for Completing the SAR Form	6	50	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: SAR Filing Tips for MSBs	4	42	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: SAR Form Completion Rate-National Overview	1	25	http://www.fincen.gov/sarreviewforweb.pdf
SAR Tips: SAR Form Preparation and Filing	1	24	http://www.fincen.gov/sarreviewforweb.pdf
SAR Tips: SAR Forms: Where to Send Completed SAR Forms	5	58	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: SAR Forms: Where to Send Completed SAR Forms	6	57	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: SAR Guidance Package	7	37	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Special Guidance Related to Identity Theft and Pretext Calling	2	34	http://www.fincen.gov/sarreview2issue4web.pdf
SAR Tips: Suspicious Activity Reporting Guidance for Casinos	7	37	http://www.fincen.gov/sarreviewissue7.pdf
SAR Tips: Terrorist-Related Activity: How to report potential terrorist-related activity	6	53	http://www.fincen.gov/sarreviewissue6.pdf
SAR Tips: Terrorist-Related Activity: How to report potential terrorist-related activity	5	55	http://www.fincen.gov/sarreviewissue5.pdf
SAR Tips: Terrorist-Related Activity: How to report potential terrorist-related activity	4	41	http://www.fincen.gov/sarreview082002.pdf
SAR Tips: Tips from the Regulators	6	54	http://www.fincen.gov/sarreviewissue6.pdf
SARs filed by Money Services Business	5	48	http://www.fincen.gov/sarreviewissue5.pdf
SARs Filed Referring to Terrorism (Prior to 09/112001 & 09/112001 through 03/31/2002)	4	25	http://www.fincen.gov/sarreview082002.pdf
SARs Filed that Refer to Terrorism (March –September 2002)	5	21	http://www.fincen.gov/sarreviewissue5.pdf
Securities Industry: SAR Analysis – Indications of Suspicious Activity	5	38	http://www.fincen.gov/sarreviewissue5.pdf
Securities and Futures Industries SARs: The First Quarter	6	23	http://www.fincen.gov/sarreviewissue6.pdf
Shell Company Activity	1	11	http://www.fincen.gov/sarreviewforweb.pdf
State and Local Law Enforcement Use of SAR Data	7	35	http://www.fincen.gov/sarreviewissue7.pdf
State and Local Law Enforcement Use of SAR Data	6	45	http://www.fincen.gov/sarreviewissue6.pdf
State and Local Law Enforcement Use of SAR Data	4	39	http://www.fincen.gov/sarreview082002.pdf

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