The SAR Activity Review

Trends Tips & Issues

Issue 2

June 2001

The SAR Activity Review

Trends

Tips &

Issues

Issue 2

Published under the auspices of the Bank Secrecy Act Advisory Group

June 2001

Table of Contents

Introduction 1

Feedback Form 2

Section 1 –SAR Statistics 4

Section 2 –National Trends and Analyses 14

1. Highlighted Trend 14
2. Other Notable Trends 18
3. Other SAR Analysis Issues 19

Section 3 –Issues with International Impact 22

Section 4 –Law Enforcement Cases 26

Section 5 –Tips on SAR Form Preparation & Filing 32

Section 6 –Issues and Guidance 35

Section 7 –Industry Forum 38

Section 8 –Index of Information Sources
Released since October 2000 40

This is a PDF version of a printed document. Although page numbers have been adjusted to provide easy navigation and electronic viewing, no information has been omitted from this publication.

Introduction

The *SAR Activity Review—Trends, Tips and Issues* is the product of a continuing dialog and close collaboration among the nation's financial institutions, federal law enforcement officials, and regulatory agencies to provide meaningful information about the preparation, use, and value of Suspicious Activity Reports (SARs) filed by financial institutions.

This publication reflects the recognition of both the relevant government agencies and the nation's financial institutions of the desirability of a continuing exchange of information between the private and public sectors to improve the SAR System. These include, among others, the American Bankers Association; Independent Bankers Association; Independent Community Bankers of America; American Institute of Certified Public Accountants; Securities Industry Association; Non-Bank Funds Transmitters Group; Federal Reserve Board; Office of the Comptroller of the Currency; Federal Deposit Insurance Corporation; Office of Thrift Supervision; National Credit Union Administration; Federal Bureau of Investigation; U.S. Department of Justice's Criminal Division, and Asset Forfeiture and Money Laundering Section; U.S. Department of Treasury's Office of Enforcement; U.S. Customs Service; U.S. Secret Service; Internal Revenue Service; and Financial Crimes Enforcement Network.

The *SAR Activity Review* is published semi-annually. The first issue was released in October 2000. Analytic reports, issue papers, and other publications related to or resulting from information contained in the *Review* may be published separately.

Questions, comments and other feedback concerning the *SAR Activity Review* are most welcome. Where possible, Email contact points are provided in the sections of the *SAR Activity Review*. A feedback form is provided on the next page. Comments may also be addressed to either or both of the *SAR Activity Review* project co-chairs:

John J. Byrne
Senior Counsel and
Compliance Manager
American Bankers Association
1120 Connecticut Ave., NW
Washington, DC 20036
(202) 663-5029 (phone)
(202) 828-5052 (fax)
jbyrne@aba.com

David M. Vogt
Assistant Director
Office of Strategic Analysis
Financial Crimes Enforcement Network
2070 Chain Bridge Road, Suite 200
Vienna, VA 22182
(703) 905-3525 (phone)
(703) 905-3698 (fax)
vogtd@fincen.treas.gov

Feedback Form

Department of the Treasury · Financial Crimes Enforcement Network

A. Please indicate your level of satisfaction with the eight sections of the SAR Activity Review.

(Circle One for Each Row)
1=Not Useful, 5=Very Useful

a.	SAR Statistics	1	2	3	4	5
b.	National Trends and Analyses	1	2	3	4	5
c.	Issues with International Impact	1	2	3	4	5
d.	Law Enforcement Cases	1	2	3	4	5
e.	Tips on SAR Form Preparation and Filing	1	2	3	4	5
f.	Issues and Guidance	1	2	3	4	5
g.	Industry Forum	1	2	3	4	5
h.	Index of Information Sources	1	2	3	4	5

B. How do you use this Report?

a. Training_____
b. Background Information Resource_____
c. Analytic Tool_____
d. Increase Management Awareness_____
e. Comparison of statistics_____
f. Make changes to your compliance program_____
g. Audit/Exam preparation_____
h. Other (identify)_____

C. Did you read the first issue (October 2000)?

a. Yes_____
b. No_____

D. If the answer to C is "Yes," did you circulate it to:

a. Your staff
b. Your colleagues
c. Senior management
d. Board/audit committee

`

E. Have you discussed the SAR Activity Review at management meetings?

F. If the answer to C is "Yes," how did you receive the Review?

a. At the ABA/ABA Money Laundering Enforcement Seminar _____
b. On an Agency's Website_____
c. From a Law or Accounting Firm_____
d. Other_____

G. Which of the following best describes your job position? (Check One)

a. [ ] CEO/COO
b. [ ] Compliance
c. [ ] Risk Management
d. [ ] Operations
e. [ ] Legal
f. [ ] Audit
g. [ ] Security
h. [ ] Government
i. [ ] Other_____

H. Any additional suggestions or comments?

_____
_____
_____
_____
_____

Thank you for your feedback.

Send your Feedback Form to:

FinCEN Office of Strategic Analysis
Fax 703-905-3698
Ora@fincen.treas.gov

or

American Bankers Association
Fax 202-828-5052
Jbyrne@aba.com

Section 1

Suspicious Activity Report Statistics[1]

April 1, 1996 - December 31, 2000

The statistics on the following pages relate to SARs filed since April 1996 by depository institutions (i.e., banks, thrifts, savings and loans, and credit unions). A small part of the total volume relates to reports filed by affiliates of depository institutions or, in some cases, filed voluntarily by brokers and dealers in securities that are not affiliated with banks, money services businesses, or gaming businesses that have no regulatory requirements at this time that mandate SAR filings.

Note: SAR statistical data is continuously updated as additional reports are filed and processed. For this reason, there may be minor discrepancies between the statistical figures contained in various portions of this report.

Exhibit 1

SAR Filings by Year and Month

	Number of Filings				
	1996	**1997**	**1998**	**1999**	**2000**
January	-	5,794	7,600	8,621	10,790
February	-	5,522	7,107	9,950	9,910
March	-	6,967	8,718	10,986	14,923
April	2,022	7,628	8,293	9,759	11,928
May	3,315	6,814	7,646	10,625	13,364
June	5,756	6,414	8,163	10,715	13,908
July	6,882	6,844	9,061	8,759	12,031
August	6,785	6,930	7696	10,014	14,846
September	6,139	7,221	8,625	8,735	13,517
October	7,269	7,486	8,223	10,049	12,662
November	5,060	6,384	7,577	10,540	14,156
December	6,297	7,593	8,223	11,753	14,896
Subtotal	**49,525**	**81,597**	**96,932**	**120,506**	**156,931**
Total Filings	**505,491**				

[1] Statistics generated for this study were based on the Document Control Number (DCN) of each record within the SAR system. The DCN is a unique number assigned to each SAR submitted. Numeric discrepancies between total number of filings and the combined number of filings of states and/or territories is a result of multiple filers listed on one or more SARs.

Exhibit 2

SAR Filings by States and Territories
—For the Period April 1, 1996 through December 31, 2000—

State/Territory	1996	1997	1998	1999	2000
Alabama	352	451	407	528	666
Alaska	63	59	132	157	347
American Samoa	2	0	7	2	10
Arizona	1,817	3,100	2,428	2,505	3,734
Arkansas	197	335	298	430	525
California	12,217	18,151	23,370	25,042	41,800
Colorado	844	1,081	1,480	1,702	1,983
Connecticut	398	785	950	4,449	4,840
Delaware	1,097	1,426	1,664	2,006	3,575
District of Columbia	166	234	281	285	456
Federated States of Micronesia	1	3	3	1	3
Florida	3,971	6,637	7,131	7,969	9,594
Georgia	869	1,504	1,688	2,205	3,039
Guam	25	80	56	84	71
Hawaii	390	535	553	575	698
Idaho	106	155	124	186	385
Illinois	1,471	2,768	2,899	3,866	4,599
Indiana	556	769	969	1,186	1,284
Iowa	251	363	326	427	450
Kansas	254	284	363	555	494
Kentucky	262	388	426	754	804
Louisiana	480	594	714	926	1,889
Maine	115	186	194	213	224
Marshall Islands	0	0	0	1	0
Maryland	615	937	1,201	1,537	2,005
Massachusetts	857	1,402	1,848	2,306	2,713
Michigan	1,119	1,717	1,858	2,753	3,678
Minnesota	950	2,263	2,212	2,513	2,714
Mississippi	152	251	222	283	507
Missouri	604	960	1,153	1,215	1,503
Montana	71	107	101	156	195
Nebraska	178	248	316	371	596
Nevada	662	1,488	2,009	2,062	3,011
New Hampshire	244	503	419	573	425
New Jersey	888	1,536	2,437	3,450	4,015

Exhibit 2 (cont.)

State/Territory	1996	1997	1998	1999	2000
New Mexico	220	237	286	314	369
New York	5,259	9,679	13,441	17,931	18,463
North Carolina	893	1,625	2,119	2,392	2,914
North Dakota	42	215	213	122	218
Northern Mariana Islands	22	5	13	33	57
Ohio	903	1,721	2,230	2,297	3,191
Oklahoma	379	497	506	698	751
Oregon	555	1,129	1,201	1,807	2,427
Overseas	12	39	7	2	22
Pennsylvania	1,452	2,482	2,544	3,571	3,363
Puerto Rico	146	562	456	316	1,047
Rhode Island	155	290	285	503	483
South Carolina	279	563	640	669	711
South Dakota	316	430	574	675	255
Tennessee	525	802	922	998	1,493
Texas	3,805	4,906	6,231	7,606	9,453
U.S. Virgin Islands	3	8	12	14	28
Unknown/Blank	318	205	28	26	249
Utah	374	882	1,114	1,384	2,175
Vermont	55	91	68	58	64
Virginia	598	1,206	1,564	1,537	1,916
Washington	753	1,766	2,192	3,147	3,325
West Virginia	109	151	161	154	167
Wisconsin	360	552	677	755	953
Wyoming	26	43	54	40	62
Total	**49,525**	**81,597**	**96,932**	**120,506**	**156,931**

Exhibit 3

Frequency Distribution of SAR Filings Ranked by States and Territories in Descending Order
—For the Period April 1, 1996 through December 31, 2000—

Rank	State/Territory	Filings (Overall)	Percentage[2] (Overall)
1	California	120,580	23.75%
2	New York	64,773	12.75%
3	Florida	35,302	6.95%
4	Texas	32,001	6.3%
5	Illinois	15,603	3.1%
6	Arizona	13,584	2.7%
7	Pennsylvania	13,412	2.65%
8	New Jersey	12,326	2.4%
9	Connecticut	11,422	2.25%
10	Washington	11,183	2.2%
11	Michigan	11,125	2.2%
12	Minnesota	10,652	2.1%
13	Ohio	10,342	2%
14	North Carolina	9,943	1.95%
15	Delaware	9,768	1.90%
16	Georgia	9,305	1.85%
17	Nevada	9,232	1.8%
18	Massachusetts	9,126	1.8%
19	Oregon	7,119	1.4%
20	Colorado	7,090	1.4%
21	Virginia	6,821	1.35%
22	Maryland	6,295	1.25%
23	Utah	5,929	1.15%
24	Missouri	5,435	1.1%
25	Indiana	4,764	Less than 1%
26	Tennessee	4,740	Less than 1%
27	Louisiana	4,603	Less than 1%
28	Wisconsin	3,297	Less than 1%
29	South Carolina	2,862	Less than 1%
30	Oklahoma	2,831	Less than 1%
31	Hawaii	2,751	Less than 1%

Exhibit 3 (cont.)

Rank	State/Territory	Filings (Overall)	Percentage[2] (Overall)
32	Kentucky	2,634	Less than 1%
33	Puerto Rico	2,527	Less than 1%
34	Alabama	2,404	Less than 1%
35	South Dakota	2,250	Less than 1%
36	New Hampshire	2,164	Less than 1%
37	Kansas	1,950	Less than 1%
38	Iowa	1,817	Less than 1%
39	Arkansas	1,785	Less than 1%
40	Rhode Island	1,716	Less than 1%
41	Nebraska	1,709	Less than 1%
42	New Mexico	1,426	Less than 1%
43	District of Columbia	1,422	Less than 1%
44	Mississippi	1,415	Less than 1%
45	Idaho	956	Less than 1%
46	Maine	932	Less than 1%
47	Unknown/Blank	826	Less than 1%
48	North Dakota	810	Less than 1%
49	Alaska	758	Less than 1%
50	West Virginia	742	Less than 1%
51	Montana	630	Less than 1%
52	Vermont	336	Less than 1%
53	Guam	316	Less than 1%
54	Wyoming	225	Less than 1%
55	Northern Mariana Islands	130	Less than 1%
56	Overseas	82	Less than 1%
57	U.S. Virgin Islands	65	Less than 1%
58	American Samoa	21	Less than 1%
59	Federated States of Micronesia	11	Less than 1%
60	Marshall Islands	1	Less than 1%

[2] All percentages are approximate.

Exhibit 4

Frequency Distribution of SAR Filings by Characterization of Suspicious Activity in Descending Order
—For the Period April 1, 1996 through December 31, 2000—

Rank	State/Territory	Filings (Overall)	Percentage[3] (Overall)
1	BSA/Structuring/Money Laundering	255,653	46%
2	Check Fraud	71,622	13%
3	Other	39,977	7.2%
4	Counterfeit Check	28,908	5.2%
5	Defalcation/Embezzlement	24,998	4.5%
6	Credit Card Fraud	24,054	4.3%
7	Check Kiting	21,306	3.85%
8	Unknown/Blank	20,963	3.8%
9	Mortgage Loan Fraud	11,703	2.1%
10	False Statement	11,416	2.05%
11	Consumer Loan Fraud	11,362	2.05%
12	Mysterious Disappearance	8,872	1.6%
13	Misuse of Position or Self Dealing	8,345	1.5%
14	Commercial Loan Fraud	4,819	Less than 1%
15	Debit Card Fraud	3,352	Less than 1%
16	Wire Transfer Fraud	3,121	Less than 1%
17	Counterfeit Credit/Debit Card	1,969	Less than 1%
18	Counterfeit Instrument (Other)	1,564	Less than 1%
19	Bribery/Gratuity	544	Less than 1%
20	Computer Intrusion[4]	65	Less than 1%

[3] All percentages are approximate.

[4] Separate box on form for this violation was added in June 2000 TD F 90-22.47, and statistics date from that period.

Exhibit 5

Frequency Distribution of SAR Filings
by Characterization of Suspicious Activity
—For the Period April 1, 1996 through December 31, 2000—

Violation	1996	1997	1998	1999	2000
BSA/Structuring/Money Laundering	20,565	35,949	47,509	61,007	90,623
Bribery/Gratuity	91	109	93	101	150
Check Fraud	8,639	13,274	13,832	16,239	19,638
Check Kiting	2,747	4,298	4,037	4,061	6,163
Commercial Loan Fraud	554	960	905	1,080	1,320
Computer Intrusion	0	0	0	0	65[5]
Consumer Loan Fraud	1,148	2,048	2,185	2,549	3,432
Counterfeit Check	2,317	4,244	5,918	7,396	9,033
Counterfeit Credit/Debit Card	385	387	182	351	664
Counterfeit Instrument (Other)	212	292	265	321	474
Credit Card Fraud	3,375	5,083	4,383	4,938	6,275
Debit Card Fraud	245	610	566	721	1,210
Defalcation/Embezzlement	3,136	5,306	5,260	5,179	6,117
False Statement	1,807	2,204	1,978	2,376	3,051
Misuse of Position or Self Dealing	914	1,537	1,645	2,063	2,186
Mortgage Loan Fraud	1,265	1,719	2,268	2,936	3,515
Mysterious Disappearance	1,168	1,767	1,855	1,857	2,225
Wire Transfer Fraud	284	499	594	772	972
Other	4,600	6,777	8,696	8,755	11,149
Unknown/Blank	1,652	2,317	2,728	7,295	6,971

[5] Separate box on the form for this violation was added in June 2000 TD F 90-22.47, and statistics date from that period.

Exhibit 6

SAR Filings by Primary Federal Regulator[6]
—For the Period April 1, 1996 through December 31, 2000—

Regulator	Total Filings by Year				
	1996	**1997**	**1998**	**1999**	**2000**
Federal Reserve Board (FRB)	5,486	9,676	10,798	14,656	17,551
Federal Deposit Insurance Corporation (FDIC)	9,839	14,908	14,735	15,883	19,255
Office of the Comptroller of the Currency (OCC)	25,072	41,722	51,879	64,946	90,141
Office of Thrift Supervision (OTS)	5,760	9,133	11,463	12,316	15,610
National Credit Union Administration (NCUA)	2,071	2,624	2,846	3,041	3,421
Unspecified	1,558	3,534	5,211	9,664	10,943

Note: In the October 2000 issue of the *SAR Activity Review*, this chart erroneously reversed the data for NCUA and OTS. The above chart corrects this error.

[6] *Unspecified* regulator indicates that the form was filed by a non-bank financial institution that is not directly supervised by one of the five agencies listed above. Such entities which have no regulatory requirements for the relevant periods that mandate SAR filings include, but are not limited to: Money Services Businesses; Insurance Companies; and Securities Brokers/Dealers who are not affiliated with banks.

Exhibit 7

Direct Referrals of SARs by Financial Institutions
To Law Enforcement[7] and Regulatory Agencies
—For the Period April 1, 1996 through December 31, 2000—

Exhibit 7 shows the number of times financial institutions that file SARs have also directly referred certain situations to law enforcement officials. The "direct referrals" in this edition of the *SAR Activity Review* have been tabulated by counting each agency to which a direct referral has been made. This method is appropriate since a situation giving rise to a single SAR can be referred to more than one agency. Such a tabulation accurately reflects the number of times particular law enforcement agencies received SAR information directly from filing institutions.

Agencies	**1996**	**1997**	**1998**	**1999**	**2000**	**Total**
Federal Law Enforcement						
Federal Bureau of Investigation	2,355	3,833	4,174	4,779	3,386	18,527
Internal Revenue Service	1,138	2,687	2,183	2,118	1,083	9,209
U.S. Secret Service	894	1,609	1,223	1,060	746	5,532
Postal Inspection Service	340	610	636	644	728	2,958
U.S. Attorney's Office	185	132	84	106	101	608
U.S. Customs Service	52	62	101	83	66	364
Department of Treasury	55	56	30	43	23	207
Drug Enforcement Administration	11	18	23	8	127	187
Naval Criminal Investigative Service/ U.S. Navy	14	18	6	17	13	68
Department of Justice	9	4	10	8	10	41
Social Security Administration (IG)	4	9	11	8	9	41
Immigration & Naturalization Service		3	12	6	11	32
Sub-Total	**5,057**	**9,041**	**8,493**	**8,880**	**6,303**	**37,774**
Other Federal Law Enforcement	**28**	**63**	**83**	**80**	**72**	**326**
Total Federal Law Enforcement	**5,085**	**9,104**	**8,576**	**8,960**	**6,375**	**38,100**
Regulatory						
Federal Deposit Insurance Corporation	24	26	25	22	42	139
Federal Reserve Board	46	29	27	13	15	130
Office of the Comptroller of the Currency	17	21	19	24	37	118

[7] Figures reflect those entities receiving five (5) or more SAR referrals. Some SARs may reference making referrals to multiple law enforcement agencies.

Exhibit 7 (cont.)

Agencies	1996	1997	1998	1999	2000	Total
Regulatory (continued)						
Securities & Exchange Commission	15	11	21	8	44	99
Office of Thrift Supervision	7	3	3	6		19
National Credit Union Administration	4	5	1	4	2	16
Federal Trade Commission				7	2	9
National Association of Securities Dealers		1	1	1	1	4
Total Regulatory	**113**	**96**	**97**	**85**	**143**	**534**
State & Local Law Enforcement						
City/Local Police Department	4,407	6,978	7,588	7,994	8,586	35,553
County/Parish	789	1235	938	1,253	1,533	5,748
D/A, A/G, or Prosecutor's Office[8]	317	445	347	401	373	1,883
State Police	181	295	263	289	329	1,357
Other State and Local	89	106	107	135	129	566
Total State & Local Law Enforcement	**5,783**	**9,059**	**9,243**	**10,072**	**10,950**	**45,107**
Other						
Pending	8	56	40	50	31	185
Unspecified	254	184	164	234	351	1,187
Private Industry[9]	29	27	33	12	15	116
Foreign Law Enforcement[10]	51	74	69	86	59	339
FinCEN/DCC	45	224	153	131	186	739
GRAND TOTAL	***11,368***	***18,824***	***18,375***	***19,630***	***18,111***	***86,308***

[8] City, County, or State.

[9] Includes referrals stating law firm, corporate security, etc.

[10] Includes referrals made to Interpol.

Section 2
National Trends and Analyses

This section of the *SAR Activity Review* outlines examples and patterns of suspicious activity reported in the national database. Some of the information has been published previously, but is included here for ease of reference.

1. Highlighted Trend

The *Highlighted Trend* for this issue of the *SAR Activity Review*—Identity Theft—was suggested by the financial industry as a topic of concern based on industry perceptions of increases in both the incidence of identity theft-based-fraud and SAR reporting about the phenomenon. Results of FinCEN's analysis of SAR data confirm these perceptions and provide insights into the patterns of criminal financial activity associated with identity theft on a national basis.

Identity Theft

In October 1998, the Congress passed the *Identity Theft and Assumption Deterrence Act of 1998* to address the problem of identity theft. Specifically, the Act amended 18 USC § 1028 to make it a federal crime for anyone to:

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

While identity theft is not a new problem, advanced technology (in particular – the Internet) is proving to be a powerful facilitator. According to the Federal Trade Commission (FTC) and law enforcement agencies, identity theft is increasing at an alarming rate. For example, in March 2000, the FTC received and responded to roughly 400 such complaints and inquiries. The FTC currently logs approximately 1,700 complaints and inquiries a week connected with all types of identity theft. Identity theft was the top consumer complaint received by the FTC during calendar year 2000. [11]

---

[11] *Washington Post*. February 4, 2001, "Your Money and Your Life," by Michelle Singletary.

SAR analysis corroborates the FTC's experience. In 1997, the first full year of required SAR reporting, 44 instances (fewer than four per month) of identity theft were reported. From January through November 30, 2000, there were 617 SARs filed (56 per month) reporting identity theft. A total of 1,030 SARs filed during the period April 1996 through November 2000 reported identity theft. Nearly half of these reports were referred to (primarily state and local) law enforcement by the filing institution.

A total of 194 financial institutions from 41 states and the District of Columbia reported some form of identity theft. California and North Carolina account for almost 30 percent of all reports of identity theft. Minnesota, Washington, and New York rank next in order for the number of SARs filed. Seventy-two percent of the retrieved SARs describe fraud perpetration in the form of check fraud, consumer loan fraud, mortgage loan fraud, credit/debit card fraud, and, to some extent, wire transfer fraud.

SAR narratives generally indicate that the most common ways to become the victim of identity theft are through the loss or theft of a purse or wallet, mail theft, and fraudulent address changes. There are also numerous instances of "insider" knowledge; i.e., persons who may share a residence, relatives, or even bank employees stealing the identity of another person. These individuals have easy access to personal information such as a checkbook bearing account numbers, Social Security Numbers (SSN) and business records. Often, the SARs do not describe how an individual perpetrator came to obtain a victim's identifying information. In the cases where a relative was involved, it was usually an adult child of the victim. SARs describe young adults applying for credit cards or bank accounts (usually via the Internet) using their parents' pertinent information except for changing the date of birth to reflect their own.

Once the perpetrator has obtained personal information, that person will open a bank account in the victim's name (or access a current account). The perpetrator will then begin depositing fraudulent, worthless or counterfeit checks into the account. Most deposits are carried out via automated teller machines (ATMs). Before checks are cleared, the perpetrator will withdraw cash on the account via ATMs. Check deposits usually average between $2,000 and $3,000 each with the total activity amounting to $20,000-$30,000. In some instances, the fraudster will deposit empty envelopes, with a dollar amount annotated, into an ATM. Once the bank detects the fraud, most of the perpetrators are discovered and turned over to law enforcement. In most instances, the bank will suffer a loss.

Numerous narratives describe the fraudulent use of another individual's SSN to obtain car loans. In most cases, the assumed SSN, along with other identifying

data, is used to purchase or lease high-end automobiles such as Jaguar, BMW, Mercedes Benz, Lexus, and sports utility vehicles. Most of the loans in this category average approximately $30,000. Loans are usually easily approved. Almost across the board, the bank becomes alerted to the scheme because the perpetrator will immediately default on the loan payments. It is a daunting task for the bank to ascertain who actually purchased/leased the vehicle in question. If the vehicle is recovered, it is normally auctioned off so that the bank can recover some of the loss.

Another common scenario described in the narratives is mail intercepts. An individual will steal an unwitting victim's mail to obtain bank checks or convenience checks issued by credit card companies. The thief will then write checks against the victim's account. The victim does not become aware of the intrusion until receipt of a monthly statement from the bank or credit card company.

Another common depiction is that of the perpetrator informing the bank of a change of address for an account holder. Once new checks are printed with the change of address they are mailed to the individual who requested the address change. Again, this goes unnoticed by the victim until the victim realizes that he/she has not received a monthly statement from the bank.

Perhaps not as common, but described enough in the narratives to warrant mentioning, are individuals preying upon the elderly either by ingratiating themselves to the person in order to obtain personal information, or by a more overt method such as pick-pocketing. Also indicated as a means of obtaining information are the use of SSNs or other personal identifiers of deceased individuals.

Some banks report fraud "rings" operating in their jurisdictions. Washington, Texas, and North Carolina banks report fraud rings apparently based in Nigeria taking over the identities of numerous customers. The members of the fraud rings deposit fraudulent checks into the accounts of these individuals, and then withdraw the money in the form of money orders or via debit cards at ATMs. A bank in Delaware uncovered a fraud ring operating out of New York. The bank identified 75 accounts that were linked by four different phone numbers. Individuals making phone calls from these numbers reported lost or stolen debit cards issued on these accounts. The bank issued new cards and convenience checks that were intercepted at JFK Airport in New York. The intercepts were accomplished by members of the fraud rings, who then redirected the cards and checks to cooperating merchants in Saudi Arabia.

Over a one-year period, a bank in North Carolina investigated 113 suspect applications for business loans. In all instances, an application for a loan of $100,000 per

business was made. Many of the applications appear to have similar handwriting or had been typed on the same typewriter. Not all of the applications have the same suspected area of fraudulent information. There are multiple irregularities in residence/business addresses, individuals' names, incorporation documents, mail drops, tax preparers, tax returns, and credit bureaus. It is suspected that most of the guarantors for these loans have been victimized by identity theft. According to the SARs filed by this bank, the bank stands to lose close to $7 million.

Another similar ring uncovered in California involved leases for as many as 400 vehicles through multiple financial institutions. The vehicles were also linked to a group dealing in large quantities of drugs. Individuals obtained leases using fraudulent income documents (primarily W-2s) then subleased the cars to individuals in other states. It appears that the ring leaders convinced unsuspecting third parties to allow their names and SSNs to be entered as signatories on the leases. The individuals signed blank credit applications and were told that by doing so they would receive a certain percentage of the profit on these investments. To date, only one vehicle has been recovered.

The FTC has developed a pamphlet to assist consumers in avoiding identity theft and, in instances of abuse, steps to take in addressing stolen identities. The pamphlet can be obtained from the FTC's website at www.consumer.gov/idtheft. In addition, the Federal banks' supervisory agencies recently released guidance to banking organizations on identity theft and pretext calling. The guidance can be found on each of the agencies' websites:

- Federal Deposit Insurance Corporation at www.fdic.gov;
- Federal Reserve Board at www.federalreserve.gov;
- National Credit Union Association at www.ncua.gov;
- Office of the Comptroller of the Currency at www.occ.treas.gov; and,
- Office of Thrift Supervision at www.ots.treas.gov.

Financial institutions should refer to Section 5 of this issue of the *SAR Activity Review* for Special SAR Form Completion Guidance Related to Identity Theft and Pretext Calling.

2. Other Notable Trends

Correspondent Accounts and Shell Company Activity

As reported in the first *SAR Activity Review*, SAR filings continue to highlight suspicious activity involving suspected shell companies — i.e., corporations that engage in no apparent business activity and that only serve as a conduit for funds or securities. The SARs indicate that many of these shell companies appear to be incorporated or registered predominantly in Delaware and to a lesser extent in Nevada, Oregon, Utah, and Wyoming. As reported in SARs, this activity often highlights substantial wire transfer activity through correspondent accounts maintained by foreign banks at U.S.-based banks.[12] In some instances, shell banks are referenced as parties to suspicious wire transfers through the correspondent accounts.

The SARs that report suspicious wire transfer activity through correspondent accounts and shell companies describe both basic and complex patterns of activity, including:

- complicated maze of unusual financial transactions;
- repetitive wire transfer patterns;
- lack of evidence of legitimate business activity;
- suspicion that shell companies are customers of a foreign bank that maintains a correspondent account at a U.S.-based bank; and,
- evidence of no business operations undertaken by the companies (as determined by due diligence exams conducted by the U.S.-based bank).

In several instances, the suspicious wire transfer activity involving shell entities and correspondent accounts has led the U.S.-based reporting bank to close its correspondent account(s) that it maintains with certain foreign-based banks.

Money Transmitter Activity

SAR filings continue to reveal suspicious financial activity involving money transmitter businesses, often those offering funds transfers to Mexico. The SARs indicate that the suspect is either the money transmitter itself, or individuals or entities using the transmitter's financial services and transaction routing networks. The activity continues to be reported by banks located throughout the

---

[12] This activity was reported prior to the release of a GAO Report entitled, Report on Correspondent Banking: A Gateway for Money Laundering, February 5, 2001, Permanent Subcommittee on Investigations and their March 6, 2001 hearing on this issue.

country. Typical observed activity includes multiple deposits (cash, checks), with occasional withdrawals, into bank accounts maintained by money transmitter businesses. Such deposits quickly accumulate into large balances. The suspicious nature of the activity is sometimes heightened by ambiguities surrounding the source of the funds, nature of the suspect's stated business(es), sudden influxes of funds, and varied multiple locations for the deposits.

Pre-paid Telephone Cards May Serve as Cover for Money Laundering

Increased SAR reporting indicates that the sale of pre-paid telephone cards may serve as a cover for money laundering in some instances. SARs filed in the last 18 months indicate that suspicious activity associated with companies and businesses involved in the sale of pre-paid telephone cards has been reported by financial institutions in fourteen states including New York, New Jersey, Texas, California, and Florida. Some of the companies and businesses involved offer other services such as check cashing, money orders, beepers, cellular phones, faxes, lottery tickets, and travel tickets. The observed activity involves frequent structured deposits and withdrawals (sometimes involving the same accounts at different bank locations) amounting to large sums over relatively brief time periods. Some scenarios involve unusual outgoing wire transfers, cashiers check purchases, check cashing activity, or check and money order deposits. Similar suspicious activities were reported during the Financial Action Task Force's (FATF) annual meeting of experts on money laundering methods and trends in December 2000.

3. Other SAR Analysis Issues

Voluntary SAR Filings

At the request of the filing industries, FinCEN conducted a study to determine the number of SARs being filed voluntarily. The initial review of the SAR database revealed that 15,139 SARs were filed by entities that appeared to fall outside of the mandatory reporting requirements. These SARs represented approximately 2.8 percent of all SARs filed for the period April 1, 1996 through December 31, 2000. For the period April 1, 1996 through December 31, 2000, casinos, using bank SAR forms, filed 55 reports. In addition, 1,062 suspicious reports were filed on the *Suspicious Activity Report by Casinos* (SARC form) by casinos located outside of Nevada (which has mandatory SAR requirements), as well as those filed by New Jersey prior to October 12, 2000 (mandatory SAR requirements for New Jersey went into effect October 12, 2000).

The initial database query was based upon the information provided in the filer field. In developing the statistics for this effort, a very broad array of search parameters was applied to identify those businesses that may be or are filing as non-depository institutions. The results were categorized by industry type such as: casino, credit/phone card services, insurance, mortgage services, money services business, realty (including property and real estate management), securities, travel, and miscellaneous.

Upon closer review, there was concern that a number of the filers identified as voluntary for the purposes of this study may have been affiliated with bank holding companies and thus subject to mandatory SAR reporting under the rules of federal banking agencies. A review of owner/subsidiary relationships confirmed that some of the filers initially identified as voluntary were in fact filed by institutions otherwise required to file. These filers were removed from the voluntary category.

The following table provides a summary of our findings relevant to voluntary SAR filings from April 1996 through December 2000.

Industry	**Number of SARs**[13]	**Referred to Law Enforcement**	**Violation Type (percentage)**
Casino SAR	55	6	BSA/Structuring/ML - 51.8% Other - 46.3%
Casino SARC	1,062	144	Structuring - 32.2% Large Transactions w/Minimal Gaming – 16.4% Money Laundering – 12.8%
Credit Card & Phone Card Service	278	87	Credit Card Fraud – 57.8% Debit Card Fraud – 17%
Insurance	120	5	BSA/Structuring/ML – 67.5% Other – 31.6%
Mortgage	169	3	Mortgage Loan Fraud – 96%
MSB	11,654	2,871	BSA/Structuring/ML – 98%
Realty/Real Estate Management	6	4	BSA/Structuring/ML – 100%
Securities, Investment, Brokerage Service	1,722	125	BSA/Structuring/ML – 73.9% Check Fraud – 9%

Industry	Number of SARs[13]	Referred to Law Enforcement	Violation Type (percentage)
Travel Services	67	65	BSA/Structuring/ML – 94%
Miscellaneous	6	2	Other – 33% False Statement – 16.6%
Total	**15,139**	**3,312**	**BSA/Structuring/ML – 91%**

[13] SARs filed from April 1, 1996 though December 31, 2000.

Section 3
Issues with International Impact

Non-Cooperative Countries and Territories—Post-Advisory SAR Analysis

On July 15, 2000, *FinCEN Advisories* were issued advising banks and other financial institutions to give enhanced scrutiny to financial transactions originating in or routed through the 15 jurisdictions that the Financial Action Task Force on Money Laundering (FATF) had also identified as "non-cooperative" in the global fight against money laundering.[14] In late January 2001, the FATF met to consider progress made by the "non-cooperative countries and territories" (NCCTs) in addressing the issues, but did not remove any jurisdiction from the NCCT list.

The following table identifies the total number of SARs filed relating to financial transactions involving each of the NCCTs during the Pre-Advisory and Post-Advisory periods.

Country	**April 1996 - July 15, 2000 (52.5 months)**	**July 16, 2000 - Nov. 30, 2000 (4.5 months)**
Bahamas	453	76
Cayman Islands	359	68
Cook Islands	4	0
Dominica	11	1
Israel	495	71[15]
Lebanon	311	54
Liechtenstein	68	12
Marshall Islands	10	3
Nauru	54	6
Niue	1	2
Panama	433	54
Philippines	566	52
Russia	847	121
St. Kitts and Nevis	55	26
St. Vincent and the Grenadines	12	2
Total	**3,679**	**548**

[14] The 15 jurisdictions are: Bahamas, Cayman Islands, Cook Islands, Dominica, Israel, Lebanon, Liechtenstein, Marshall Islands, Nauru, Niue, Panama, Philippines, Russia, St. Kitts and Nevis, and St. Vincent and the Grenadines.

[15] Period 7/16/00-11/16/00.

Of the 548 SARs filed relating to financial activities involving the NCCTs during the post-advisory period, 75 percent cited BSA/Structuring/Money Laundering as the alleged violation. Most of that activity described wire transfer activity either to or from the NCCT. Other foreign countries or territories mentioned in the SARs relating to transactions involving the NCCTs included Latvia, Cyprus, Switzerland, Austria, Hong Kong, Antigua, British Virgin Islands, Isle of Man, Belize and the Dominican Republic. Dollar amounts involving wire transfers were high – often involving millions of dollars. Commercial loan fraud was cited as the alleged violation in all of the SARs filed with violation amounts greater than $100 million. Approximately 10 percent of the total number of SARs filed were referred to law enforcement directly by the filing financial institution.

FATF Typologies Exercise

On December 6-7, 2000, the FATF held its annual meeting of experts on money laundering methods and trends in Oslo, Norway. These FATF typologies exercises provide a venue for law enforcement and regulatory experts to identify and describe current money laundering methods and trends, emerging vulnerabilities, and potential countermeasures. The major issues examined by the group of experts included on-line banking and Internet casinos; trusts, and other non-corporate vehicles and money laundering; lawyers, notaries, accountants and other professionals; the role of cash vs. other payment methods in money laundering schemes; and terrorist financing. A number of countries provided case examples based on the filings of unusual or suspicious activity reports. The *FATF Report on Money Laundering Typologies 2000-2001,* can be found at www.oecd.org/fatf or FinCEN's website at www.treas.gov/fincen.

Multilateral Illicit Currency Flows Study

Action Item 4.5.3 of the National Money Laundering Strategy for 2000 (NMLS) calls for mechanisms and processes associated with the movement of criminal proceeds into, through, and out of the United States and other at-risk nations. In January 2001, agreement was reached in principle with a Core Group of nations represented in the Egmont Group of Financial Intelligence Units and other interested countries to explore the feasibility of jointly analyzing illicit currency movements over large geographic areas. Discussions involving the Core Group (comprised of nations in the Americas, Western Europe, Eastern Europe, Middle East, East Asia, and South Asia) centered on the potential utility of aggregate suspicious/unusual transaction data reported by financial institutions in identifying and tracking the movement of criminal proceeds into, out of, and/or through individual

nations and geographic areas. Core Group representatives[16] agreed to continue discussions on both a bilateral and multilateral basis with the goal of initiating a joint process for analyzing and sharing information reflecting illicit currency movements.

Egmont Group – Strategic Analysis Initiative

In June 2001, the Egmont Group of Financial Intelligence Units (FIUs) will hold its Ninth Plenary meeting in the Hague. FinCEN will organize a workshop on Strategic Analysis/Illicit Currency Flows with assistance from the FIU in Italy. FinCEN will make a presentation on the methodology and results of the findings from its correlation of SARs, Currency Transaction Reports (CTRs), and Reports of International Transportation of Currency or Monetary Instruments (CMIRs) relating to a particular NCCT. A representative of Italy's FIU, Ufficio Italiano dei Cambi, will present findings from their statistical analysis study of illicit currency flows between Italy and the NCCTs. A formal process, within the Egmont Group, for the exchange of strategic trend and pattern information may develop from these discussions.

Global Use of SARs

Sweden: Sweden's FIU reports that there were 2,560 suspected cases of money laundering reported to the FIU during 2000, which constitutes a 70 percent increase from 1999.[17] ("Suspected cases" are defined as those reports of unusual/suspicious activity required to be reported by banks, credit companies, exchange offices, insurance brokers and life insurance companies.) Almost 70 percent of the reports were made by exchange offices, while 22 percent were from banks. Analysis of those suspected cases resulted in 49 preliminary investigations.

Belgium: The Financial Information Processing Unit (CTIF) is an independent administrative authority that receives and analyzes unusual or suspicious activity reported by more than 15,000 individuals or companies in Belgium. Between December 1, 1993 and June 30, 2000, the Unit received 42,302 suspicious transaction reports. Of those suspicious transaction reports, 26,197 reports were transmitted to the Public Prosecutor's Office. During that same period, the Unit

---

[16] The Core Group of countries identified as interested in participating in the study included Canada, Italy, Japan, Thailand, Israel, Latvia, Croatia, and the Netherlands. Other countries that may be interested in participating in the study include Australia, Mexico and Brazil.

[17] As reported in the Financial Intelligence Unit's Annual Report 2000, Criminal Investigation Service, Criminal Intelligence Unit, Stockholm, Sweden.

opened a total of 8,094 case files, of which 2,580 were turned over to the Crown Prosecutor. Of those case files, 177 gave rise to criminal sentences, 67 were brought before the correctional courts and 13 were turned over for disposition to foreign judicial authorities.[18]

Estonia: Between July 1, 1999, when Estonia's Money Laundering Information Bureau was created, and March 22, 2001, 632 disclosures of unusual or suspicious transactions and information requests from other countries were received. Of those, 37 cases were forwarded to the police or tax authorities for investigation. Twelve criminal investigations have been initiated. One case has been decided in court. One person has been convicted. [19]

The following table identifies the unusual and suspicious transaction reports and information requests from other countries submitted to Estonia's Money Laundering Information Bureau by type of filer:

Statistics by Initiators	**1999**[20]	**2000**	**2001**[21]	**Total**
Banks	22	327	152	501
Police authorities	16	16	5	37
Foreign countries	10	19	11	40
Customs	3	5	2	10
Tax Department	1	2	3	6
Currency Exchange	0	7	2	9
Lawyers	0	1	1	2
Others	4	17	6	27
Total	56	394	182	632

The Netherlands: During 1999, the Netherlands' Office for the Disclosure of Unusual Transactions (MOT) received 45,079 reports of unusual transactions, up from 19,303 reports of unusual transactions received in 1998. Of the 45,079 reports, 67 percent were received from exchange offices, 28 percent from banks. Of these reports, 10,803 or 24 percent were passed to the police for further investigation.[22]

---

[18] 1999/2000 Annual Report of the Financial Information Processing Unit in Belgium. (CTIF)
[19] Presentation to Eighth Egmont Plenary in 2000 and updated via email.
[20] Statistics reflect reports received between July 1, 1999 and December 31, 1999.
[21] Statistics reflect reports received between January 1, 2001 and March 22, 2001.
[22] Office for the Disclosure of Unusual Transactions 1999 Annual Report and 2000 Annual Report.

Section 4
Law Enforcement Cases

This section of the *SAR Activity Review* provides law enforcement agencies the opportunity to summarize investigative activity in which SARs and other BSA information played an important role in a successful investigation and/or prosecution of criminal financial activity. Each subsequent issue of the *SAR Activity Review* will include new examples based on information received from law enforcement during the preceding six months.

SAR Filing Leads to Identification of Elaborate Ponzi Schemes

Case one— A multi-agency investigation of several subjects engaged in a Ponzi scheme, in which 5,000 investors were defrauded of $67 million, was aided by the filing of a SAR by a financial institution in Hawaii. Proceeds of the scheme were deposited into numerous accounts at various business locations in Hawaii and then wire transferred to offshore accounts in Antigua, Bahamas and Vanuatu. The scheme collected approximately $67 million from about 5,000 investors throughout the United States and several foreign countries. Investors were told that their money would be invested with the Cayman Islands Government, which would pay the principals 20 percent interest per week. The principals, in turn, promised a return of 8 percent per week, plus 3 percent referral fee for investors who enrolled new investors. The investment was to run on a 13-week cycle. In reality, there was no such investment with the Caymanian Government, and the defendants kept substantial profits.

As reported in the SAR, one of the defendants deposited $100,000 which was subsequently wire transferred to Ireland. The cash consisted of $95,000 in one hundred dollar bills and $5,000 in twenty dollar bills. The customer represented himself as an investment consultant and a self-employed educational systems marketer. The customer provided bank officials with useful identification documents, and even inquired of bank employees if they wanted to invest with him promising to pay them a high rate of return. The transaction indicated that the customer was working as a middle person to hide illegitimate income from other people who may have been investors under his control.

Thus far, three search warrants have been executed and $1,473,536 has been seized. One defendant pled guilty to six counts of money laundering, mail fraud, wire fraud, conspiracy to launder monetary instruments, and conspiracy to defraud the United States. Six additional defendants were named in a 100-count

indictment charging them with mail fraud, wire fraud, money laundering, structuring, and conspiracy. Indictments of other individuals involved in this scheme are expected. *(Source: U.S. Customs Service)*

Case two— An FBI investigation was predicated on a SAR filed by a bank in Indiana that indicated structuring of currency deposits. After further investigation, an elaborate Ponzi scheme was identified which had been in operation from 1996 through August 2000. More than 500 victims were defrauded of more than $40 million before the scheme was discovered. This case was worked jointly with the Internal Revenue Service (IRS), the Securities and Exchange Commission (SEC), and the U.S. Marshals Service. The subject fled to Mexico where he was arrested. The subject, charged with 20 counts of money laundering and 11 counts of mail fraud, is currently incarcerated and awaiting trial. This investigation could be the largest financial loss case to be successfully investigated and presented by the Southern District of Indiana. *(Source: FBI)*

Case three— After review of a SAR filed by a Michigan bank, the IRS initiated an investigation on an individual who engaged in a Ponzi scheme. The SAR, which was filed on an associate of the principal defendant, described allegedly fraudulent activity involving the sales of multi-year contracts for satellite dish systems and services to individuals. The customers were promised that their funds would be deposited in offshore accounts to help offset the cost of the satellite services. A business identified in the SAR narrative as being involved with the offshore investment activity was owned by the principal defendant.

The investigation led to the indictment of the defendant on 63 counts of mail fraud, wire fraud, and money laundering. Subsequently, the defendant entered a plea to one count of mail fraud and one count of money laundering. The defendant admitted that he solicited over $1.2 million from over 105 investors from late 1994 through September 1997 by representing that he could place the funds in secure overseas investments, which would return at least six times the investment amount in 40 weeks. In fact, the defendant placed the funds in the business account of the company identified in the SAR's narrative. He admitted that he used the funds from this account to purchase 20 vehicles for cash, which he used or gave to friends. He drew funds to pay salesmen who recruited other investors. He used approximately $300,000 of investors' money to make purchases of furniture, an entertainment center, firearms, real estate, and other items. The defendant was sentenced to a substantial jail sentence, and the government seized numerous assets including 10 vehicles, which were sold for approximately $200,000. *(Source: IRS/Criminal Investigation)*

SAR Filings Lead to Investigation Involving Black Market Peso Exchange

An FBI investigation was initiated upon the receipt of a SAR from a bank in New York that identified deposits being structured to avoid the filing of CTRs. This case was worked jointly with the FBI, New York City Department of Investigation, IRS, and U.S. Customs Service. Over 80 SARs were filed by New York area banks and identified over 179 deposits in amounts just under $10,000. The investigation revealed that the source of funds was the Colombian drug cartel. The proceeds of drug sales were deposited into bank accounts and regularly withdrawn by means of either cashiers' checks or wire transfer and forwarded to various companies throughout the United States. The funds were used to pay for products to be shipped to Colombia. Ten individuals were arrested. The primary subject fled to another country. *(Source: FBI)*

SAR Filings Unveil Fraudulent Securities Dealer

Two SARs filed by a central Florida bank resulted in the initiation of a money laundering investigation of a fraudulent securities dealer operating a prime bank fraud scheme. The SARs reported unusual account activity and international wire transfers in the tens of millions of dollars. The case resulted in the identification of the account holder who had an extensive criminal history of fraud scheme activity. The bank accounts identified in the SARs, with a combined balance of $10.8 million, were subsequently seized. A search warrant was executed on the defendant's business and his recently purchased vehicle was seized. It is anticipated that the monies seized will be subject to petition by innocent victims of this fraud scheme. *(Source: U.S. Customs Service)*

SAR Filing Leads to Embargo Investigation

An investigation of a possible violation of the International Emergency Economic Powers Act was initiated following the filing of a SAR by a bank in New York. The SAR stated that an unnamed bank vice president in charge of the funds transfer program manipulated four payments to the Sudan totaling $73,000 in violation of the embargo. The subject allegedly manipulated the bank's internal Office of Foreign Assets Controls (OFAC) filtering system by either manually over-riding its function (to screen and block any and all funds transfers in violation of OFAC laws and regulations) or by omitting any reference to Sudan and re-processing the wire transfers through the same filtering system. The case was subsequently turned over to OFAC for appropriate action. *(Source: U.S. Customs Service)*

SAR Filing Results in Arrests on Drug Trafficking and Money Laundering

A multi-agency money laundering/marijuana trafficking investigation was initiated following the filing of a SAR by a bank in Tennessee. The SAR disclosed that an individual was depositing large amounts of U.S. currency into three bank accounts. The deposits ranged from $5,000 to $25,000 with the majority of the deposits consisting of one hundred dollar bills. Approximately $1.2 million was deposited into these accounts during a one-year period. Thus far, seven defendants have been indicted on multiple counts of money laundering and marijuana trafficking. Two of the defendants have pled guilty and are awaiting sentencing. *(Source: U.S. Customs Service)*

SAR Filing Locates Check Kiting Suspect

An investigation into the exportation of stolen merchandise exposed that the defendant was using a check kiting scheme to defraud local area banks resulting in losses exceeding $50,000. Subsequent to the defendant's bond hearing, the defendant fled the jurisdiction and continued to engage in criminal activity. A SAR filed by a Washington bank enhanced the investigation by identifying his aliases, which led to locating the fugitive. The SAR identified other accounts belonging to the defendant and detailed his check kiting scheme, which involved the use of accounts and checks issued in fictitious names. The defendant was arrested and deported. *(Source: U.S. Customs Service)*

Travel Agent Convicted

An IRS investigation in Virginia was initiated on the owner of a travel agency for currency structuring charges after the analysis of SAR and CTR filings. In addition to the travel agency, the defendant operated a money transmittal business that was wiring funds to his business interests in Lima, Peru, and Bogota, Colombia. An analysis of subsequent SARs and CTRs, coupled with various investigative techniques, including the execution of several search warrants, led to the defendant entering a plea to one count of money laundering. The defendant admitted structuring three transactions so that he would not trigger the filing of a CTR. The defendant structured deposits totaling between $2.5 to $5 million and used six business accounts at five financial institutions to facilitate his activities. The defendant consented to the administrative forfeiture of $10,000 seized from his business accounts. *(Source: IRS/Criminal Investigation)*

Three Individuals Convicted in Phantom Bank Scheme

The IRS-Criminal Investigation and the FBI conducted an investigation of several individuals involved in soliciting investments and deposits in a financial institution that falsely claimed Indian tribal authority and offshore-style banking privacy. The defendants used the Internet to solicit potential customers to open accounts with this phantom financial institution. The defendants obtained in excess of $7 million from investors and depositors through false representations. Depositors and investors of this phantom financial institution were solicited to invest almost $3 million in worthless railroad bonds. Subsequently, a portion of the funds was diverted into the defendants' personal bank accounts. An analysis of SARs assisted the government in obtaining convictions of the defendants in the Western Judicial District of Oklahoma of mail fraud, wire fraud, money laundering and tax crimes charges. *(Source: IRS/Criminal Investigation)*

SARs Lead to Conviction of Major Cocaine Trafficker

A joint investigation conducted by the IRS/CID, DEA, and the Bureau of Alcohol, Tobacco, and Firearms (ATF) was initiated by an analysis of SARs and CTRs filed by banks in Ohio. Two SARs led investigators to accounts that had over $1 million of cash deposits. A search warrant for the defendants' residence resulted in the seizure of over $300,000 in cash, two vehicles, seven firearms (including an AK-47), and jewelry valued at $100,000. The investigation culminated with a 31-count indictment on a husband and wife on charges including conspiracy to distribute cocaine, money laundering, and tax fraud. Each defendant was convicted on multiple counts and sentenced to serve jail time. The defendants were fined $12,500, ordered to pay a substantial amount of back taxes to the IRS, and they forfeited numerous assets including $327,126 in cash, luxury automobiles, and numerous items of jewelry including four Rolex watches. *(Source: IRS/Criminal Investigation)*

Major Credit Card Thief Convicted

On February 15, 2000, an individual from New York pled guilty to three felony charges of money laundering, interstate transportation of stolen property, and credit card fraud. The defendant obtained access to fitness centers and country clubs across the country, stealing credit cards from gym lockers. The defendant charged thousands of dollars in merchandise, including computers, stereo equipment and Rolex watches and resold the merchandise to individuals who had previously placed orders with the defendant. The investigation was initiated from

a referral from local law enforcement authorities. Various investigative techniques, including the analysis of CTR and SAR filings and the execution of a search warrant ultimately led to the defendant's conviction. The defendant was sentenced to serve 50 months and ordered to make restitution of $782,298. Agencies participating in this investigation with local law enforcement included the IRS-Criminal Investigation, FBI, and the U.S. Secret Service. *(Source: IRS/ Criminal Investigation)*

SAR Unveils Network of Brazilians Involved in a Stolen Check Scheme

A SAR filed by a financial institution in Pennsylvania led to a joint investigation by the IRS/Criminal Investigation, the U.S. Postal Inspection Service, and the FBI into a network of Brazilian nationals that used U.S. banks to launder the proceeds generated from stolen checks. Additional SARs were filed by financial institutions throughout the United States that identified the eleven co-conspirators charged with money laundering. Checks for individuals and companies located in South America were fraudulently endorsed and deposited into more than 150 bank accounts at approximately 50 different financial institutions in Pennsylvania, New Jersey, Maryland, New York, Massachusetts, Florida, Illinois, Wisconsin, Ohio, Virginia, New Hampshire, and Iowa. Those accounts had been opened with false identification, such as drivers' licenses, passports, and social security cards. The main conspirator received a sentence of 31 months in custody, followed by three years of supervised release, and was ordered to pay $255,421 in restitution. Three individuals remain fugitives. *(Source: IRS/Criminal Investigation)*

Section 5
Tips on SAR Form Preparation & Filing

SARs are *properly filed* with the Internal Revenue Service's Detroit Computing Center. Paper SARs should be addressed to: IRS Detroit Computing Center, FinCEN, P.O. Box 33980, Detroit, MI 48232-0980. Magnetic Media Diskettes should be mailed to: IRS Detroit Computing Center, FinCEN, 985 Michigan Avenue, Detroit, MI 48226. Questions on how to complete the SARs should be directed to the appropriate regulator or to FinCEN's Regulatory Help Line at 800-949-2732.

The Importance of the Narrative

The information obtained from the filing of SARs plays an important role in identifying potential illegal activities, such as money laundering, and it assists in the detection and prevention of the flow of illicit funds through our financial system. For these reasons, it is critical that the information conveyed in SAR filings be as accurate and complete as is possible. In particular, Part V of the Suspicious Activity Report TD F 90-22.47 revised in June 2000 (the narrative) should identify the essential elements of information or the ***who, what, where, when, and why*** of the suspicious activity. The narrative should be a chronological and complete account of the possible violation of law.

To assist the filer in providing the most complete description of the suspect activity, we suggest the following tips:

- ***Who*** is conducting the activity? While Part II calls for suspect information, the narrative can be used to further describe the known information about the suspect(s), including occupation or nature of the suspect's business(es). If more than one individual or business is involved in the suspicious activity, identify all suspects and any known relationships among them in the narrative section. While detailed suspect information may not always be available (*e.g.,* in situations involving non-account holders), such information should be included to the maximum extent possible.

- ***What*** instruments or mechanisms are being used in the transaction(s)? An illustrative list of instruments that could be used in suspicious activity includes, but is not limited to: wire transfers, letters of credit and other trade instruments, correspondent accounts, casinos, structuring, shell companies, bonds/notes, stocks, travelers checks, bank drafts, money orders, etc.

- ***Where*** did the suspicious activity take place? Identify all bank accounts[23] involved in the suspicious activity. Use the narrative section to indicate if multiple branches of a single financial institution were involved in the suspicious activity. Specify if the suspected activity or transactions involve a foreign jurisdiction. If so, indicate the foreign jurisdiction[24] involved in or affiliated with the suspected activity or transaction(s).

- ***When*** did the suspicious activity take place? If the pattern of activity has been occurring over a period of time, state when the suspicious activity was first noticed and the duration of activity. Often times, filers will provide a tabular presentation of the suspicious account activities (wires in and out). While this information is useful, do **not** insert objects, tables, or pre-formatted spreadsheets in the narrative to describe the suspicious activity. Objects, tables, and pre-formatted spreadsheets do not convert properly when being input into the SAR database.

- ***Why*** does the filer think the activity is suspicious? We suggest that you describe in a few words, your industry/business — bank, credit union, thrift, savings and loan, casino, mortgage broker, travel services, insurance, real estate, investment services, money remitter, check casher, etc. Then, describe as fully as possible why the activity or transaction is unusual for that customer. Some common patterns of suspicious activity could include, among others:

  - A lack of evidence of legitimate business activity, or any business operations at all, undertaken by many of the parties to the transaction(s);
  - Unusually large numbers of wire transfers;
  - Unusually complex series of transactions;
  - Transactions conducted in bursts of activities within a short period of time; and,
  - Beneficiaries maintaining accounts at foreign banks that have been subjects of previous SAR reporting due to suspicious wire transfer activity.

It is important that the narrative contain a full picture of the suspicious activity involved. For example, if what appears to be structuring of currency deposits is matched with outgoing wire transfers from the accounts, the SAR narrative should include information about both the structuring and information about the outbound transfers (including their amounts and beneficiaries of the funds transfers).

---

[23] When more than four bank accounts are involved in the suspect activity, use the narrative section of the SAR to identify those additional bank account numbers not already identified in Part I, Item 14.

[24] If activity is identified as suspicious and it involves a transaction from a country or jurisdiction for which enhanced scrutiny reporting guidance has been issued (for instance, NCCTs), then identify the country or jurisdiction in the narrative.

Special SAR Form Completion Guidance Related to Identity Theft and Pretext Calling

Criminal activity related to identity theft or pretext calling has historically manifested itself as credit or debit card fraud, loan or mortgage fraud, or false statements to the institution, among other things. As a means of better identifying and tracking known or suspected criminal violations related to identity theft and pretext calling, a banking organization should, in addition to reporting the underlying fraud (such as credit card or loan fraud) on a SAR, also indicate within the narrative of the SAR that such a known or suspected violation is the result of identity theft or pretext calling. Specifically, when identity theft or pretext calling is believed to be the underlying cause of the known or suspected criminal activity, the reporting institution should, consistent with the existing SAR instructions, complete a SAR in the following manner:

- In Part III, Box 35, check all appropriate boxes that indicate the type of known or suspected violation being reported and, in addition, in the "Other" category, write in "Identity Theft" or "Pretext Calling," as appropriate.

- In Part V, explain what is being reported, including the grounds for suspecting identity theft or pretext calling in addition to the other violation being reported.

- In the event the only known or suspected criminal violation detected is the identity theft or pretext calling, then write in "Identity Theft" or "Pretext Calling," as appropriate, in the "Other" Category in Part III, Box 35. Provide a description of the activity in Part V of the SAR.

Section 6
Issues & Guidance

This section of the *SAR Activity Review* discusses current issues of common interest raised with regard to the preparation and filing of SARs. The discussion is intended to identify SAR-related issues and provide explanations so that filing organizations can reasonably address these issues. This section represents the collective opinions of the government agencies that require organizations to file SARs.

Filing SARs on Continuing Activity after Law Enforcement Contact

Questions have been raised regarding the necessity for the continued filing of SARs on continuing activity after law enforcement has contacted a financial institution with regard to a SAR filing. In some instances, after the filing of one or more SARs, law enforcement has contacted a financial institution requesting more specific information with regard to the suspect activity or requesting identified supporting documentation. In other instances, a law enforcement agency has contacted a financial institution to report that it does not intend to investigate the matter reported on the SAR.

If conduct continues for which a SAR has been filed, the guidance set forth in the October 2000 *SAR Activity Review* (Section 5 - Repeated SAR Filings on the Same Activity) should be followed even if a law enforcement agency has declined to investigate or there is knowledge that an investigation has begun. The filing of SARs on continuing suspicious activity provides useful information to law enforcement and supervisory authorities. Moreover, the information contained in a SAR that one law enforcement agency has declined to investigate may be of interest to other law enforcement agencies, as well as supervisory agencies.

Filing SARs on Activity Outside the United States

Consistent with the SAR regulations, it is expected that financial institutions will file SARs on activity deemed to be suspicious even when a portion of the activity occurs outside of the United States or the funds involved in the activity originated from outside the United States. Although foreign-located operations of U.S. organizations are not required to file SARs, an organization may wish, for example, to file a SAR with regard to suspicious activity that occurs outside of the United States that is so egregious that it has the potential to cause harm to the entire organization. (It is, of course, expected that foreign-located operations of

U.S. organizations that identify suspicious activity will report such activity consistent with local reporting requirements in the foreign jurisdiction where the operation is located.)

Prohibition on Notification

As set forth in the October 2000 *SAR Activity Review* (Section 5 - Disclosure of SARs and Underlying Suspicious Activity), federal law (31 U.S.C. 5318(g)(2)) prohibits the notification to any person that is involved in the activity being reported on a SAR that the activity has been reported. This prohibition extends to disclosures that could indirectly result in the notification to the subject of a SAR that a SAR has been filed, effectively precluding the disclosure of a SAR or even its existence to any persons other than appropriate law enforcement and supervisory agency or agencies. Self-regulatory organizations such as the New York Stock Exchange and the National Association of Securities Dealers are not appropriate supervisory agencies under current law for purposes of SAR disclosure by financial institutions. This prohibition does not preclude, under federal law, a disclosure in an appropriate manner of the facts that are the basis of the SAR, so long as the disclosure is not made in a way that indicates or implies that a SAR has been filed or that information is included on a filed SAR.

In the rare instance when suspicious activity is related to an individual in the organization, such as the president or one of the members of the board of directors, the established policy that would require notification of a SAR filing to such an individual should not be followed. Deviations to established policies and procedures so as to avoid notification of a SAR filing to a subject of the SAR should be documented and appropriate uninvolved senior organizational personnel should be so advised.

The prohibition on notification of a SAR filing can raise special issues when SAR filings are sought by subpoena or court order. The SAR regulations direct organizations facing these issues to contact their primary supervisor, as well as FinCEN, to obtain guidance and direction on how to proceed. In several matters to date, government agencies have intervened to ensure that the protection for filing organizations and the integrity of the data contained within the SAR database remain intact.

Disclosure of SAR Documentation

Under the SAR regulations, institutions filing SARs should identify within the SAR, and are directed to maintain all "supporting documentation" related to the activity being reported. Disclosure of supporting documentation related to the

activity that is being reported on a SAR does not require a subpoena, court order, or other judicial or administrative process. Under the SAR regulations, financial institutions are required to disclose supporting documentation to appropriate law enforcement agencies, or FinCEN, upon request.

Applicability of Safe Harbor

The safe harbor provisions applicable to SAR filings provide a safe harbor for organizations that provide a SAR to all authorized government personnel, including Federal, state, and local authorities. Similarly, the safe harbor provisions apply even if the report of activity that is a possible violation of law or regulation is made orally or in some form other than through the use of a SAR.

Section 7
Industry Forum

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

In this issue, David Wittman of First Data Corporation/Western Union provided the following information.

1. **Although there are new regulations that have been issued requiring Money Services Businesses to report suspicious activity for transactions occurring after January 1, 2002, can an MSB report transactions before then and how?**

The government has always encouraged voluntary reporting of suspicious activity. Some of the national MSBs, including the leading money transmission services, money order and traveler's checks issuers, and currency exchange providers have already developed sophisticated internal systems to detect suspicious activity and have a long record of cooperation in assisting law enforcement in the effort to prevent money laundering. Until the Suspicious Activity Report form for MSBs is finalized, we use the Suspicious Activity Report form revised June 2000.

2. **Are MSBs that report suspicious transactions prior to January 1, 2002 afforded the same "safe harbor" protection as banks?**

We rely on 31 USC 5318(g)(3), which provides that any financial institution that reports possible violations of law will not be liable for such disclosure.

3. **Based on a customer's account activity, banks can monitor their customers' accounts for unusual or suspicious transactions. Money transmitters do not have an account or on-going relationship with many of their customers. How can they determine whether a customer's transaction activity is unusual or suspicious?**

Many of the leading Money Service Businesses have already developed sophisticated programs to detect suspicious activity. Key components of these programs include "Know Your Customer" principles such as requiring identification of specific information about large transactions including the purpose of the transaction

and the relationship between the sender and payee. Other tools include transaction activity reports which help detect possible structured activity or suspicious transactions. Additionally, over the past several years, these businesses have increased training and communication to their employees and sales outlets on detecting and reporting suspicious activity.

4. **Most money orders and some traveler's checks are purchased anonymously (since there is no requirement to verify the purchaser's identity) nor is the payee information recorded on the instrument at the time of purchase. Additionally, some money orders are sold through third-party sales outlets. Absent being able to identify the purchaser or payee, or having visibility to the purchase of the instrument, how can a money order or traveler's check issuer identify suspicious activity?**

Some issuers have implemented automated monitoring systems on the clearing and reconciliation side. Specifically, these types of programs identify groups or series of items that appear to have been deposited together at a particular bank or financial institution. These items are then generally reviewed manually to determine if they may have been purchased by the same individual at different locations, were purchased by different individuals and were deposited into a single account, or if the items appear to have unusual markings or are otherwise suspicious.

Section 8

Index of Information Sources Released since October 2000

As a result of recommendations of the BSA Advisory Group SAR Feedback Subcommittee, this and future issues of the *SAR Activity Review* will include an index of information sources released since the issuance of each previous report.

U.S. Government Reports:

Suspicious Banking Activities, Possible Money Laundering by U.S. Corporations Formed for Russian Entities, U.S. General Accounting Office, Report to the Ranking Minority Member, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate. GAO-01-120, October 31, 2000. Document can be found at www.gao.gov.

Bank Regulators' Evaluation of Electronic Signature Systems, U.S. General Accounting Office, Letter to Chairman Alan Greenspan, Board of Governors of the Federal Reserve System and John D. Hawke, Jr., Comptroller of the Currency. GAO-01-129R Electronic Signature Systems. Document can be found at www.gao.gov.

Minority Staff of the Permanent Subcommittee on Investigations, Report on Correspondent Banking: A Gateway for Money Laundering, February 5, 2001. Document can be found at www.senate.gov/~gov_affairs/020501_psi_minority_report.htm.

International Narcotics Control Strategy Report, March 1, 2001, Department of State. Document can be found at www.state.gov.

Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption, issued by the Department of Treasury, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the Department of State, January 16, 2001. Document can be found at www.treas.gov/press/releases/guidance.htm.

Bank Secrecy Act/Anti-Money Laundering, Comptrollers Handbook, Office of the Comptroller of the Currency, Consumer Compliance Examination, Revised for Web Publication, December 2000. Document can be found at www.occ.treas.gov/handbook/compliance.htm.

Reports from International Organizations:

Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2000-2001, February 1, 2001, FATF-XII. Document can be found at www.oecd.org/fatf.

OECD/FATF Public Statement, Progress Report on Non-Cooperative Countries and Territories, February 1, 2001. Document can be found at www.oecd.org/fatf.

Review of FATF Anti-Money Laundering Systems and Mutual Evaluation Procedures 1992-1999 (February 15, 2001). Document can be found at www.oecd.org/fatf.

A Manual of Best Practice for Combating Money Laundering in the Financial Sector. Economic Paper No 43. Commonwealth Secretariat. January 2001. Document can be found at www.thecommonwealth.org.

Wolfsberg Anti-Money Laundering Principles, Transparency International, October 30, 2000. Document can be found at www.transparency.org.

Reports from Foreign Governments:

Financial Services Authority of the United Kingdom, Money Laundering: The FSA's New Role, Policy Statement on Consultation and Decisions on Rules, January 2001. Document can be found at www.fsa.gov.uk.

Fighting Money Laundering in the UK: NCIS Financial Investigators Conference, 30/00, November 6, 2000. Document can be found at www.ncis.gov.uk.

Advanced Fee Schemes Can Affect Anyone, West African Organized Crime Section, NCIS/UK, March 2, 2001. Document can be found at www.ncis.gov.uk.

AUSTRAC 1999-2000 Annual Report, October 2000. Document can be found at www.austrac.gov.au.

Belgian Financial Information Processing Unit, 2000 Annual Report. Document can be found at www.ctif-cfi.be.

Sweden's Financial Intelligence Unit Annual Report 2000, Criminal Investigation Service, Criminal Intelligence Unit. Document can be found at www.cis.ciu.gov.sw.

Money Laundering Report, Office Switzerland/Federal Office for Police, 2nd Annual Report. Document can be found at www.admin.ch/bap.