The SAR Activity Review

Trends

Tips &

Issues

Issue 3

October 2001

The SAR Activity Review

Trends

Tips &

Issues

Issue 3

Published under the auspices of the Bank Secrecy Act Advisory Group

October 2001

Table of Contents

Introduction 1

Feedback Form 3

Section 1 –SAR Statistics 5

Section 2 –National Trends and Analyses 15

1. Highlighted Trend 15
2. Other Notable Trends 17
3. Other SAR Analysis Issues 25

Section 3 –Issues with International Impact 27

Section 4 –Law Enforcement Cases 29

Section 5 –Tips on SAR Form Preparation & Filing 37

Section 6 –Issues and Guidance 43

Section 7 –Industry Forum 45

Section 8 – Mailbag 49

Appendix 1– Characterization of Suspicious Activity by States/Territories by Year 51

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. Because of the recent terrorist attacks against the United States, this issue of the *SAR Activity Review* includes a section to assist financial institutions in reporting suspicious transactions that may be related to terrorist activities. (See Section 6)

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 sector to improve the SAR System. These financial institutions and government agencies 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 semiannually. The first issue was released in October 2000, the second in June 2001. Analytic reports, issue papers, and other publications related to or resulting from information contained in the *SAR Activity Review* may be published separately.

As a result of questions raised since the first *SAR Activity Review* was published, we have added a new Section called "Mailbag." This section will answer questions about the use and utility of the SAR data and other issues raised by the industry that do not require full policy discussions like those in Section 6, "Issues and Guidance."

Questions, comments and other feedback concerning the *SAR Activity Review* are most welcome. A feedback sheet is included on page 3. 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
(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. Mailbag	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. Did you read the second issue (June 2001)?

a. Yes_____
b. No_____

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

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

`

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

G. If the answer to C or D 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_____

H. 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_____

I. 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 – April 30, 2001

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 who are not affiliated with banks; money services businesses; or gaming businesses that, at this time, are not yet required under the Bank Secrecy Act (BSA) to file SARs.

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 the various portions of this report or in previous reports.

Exhibit 1
SAR Filings by Year and Month

	Number of Filings					
	1996	**1997**	**1998**	**1999**	**2000**	**2001**
January	-	6,123	6,832	8,621	13,399	13,767
February	-	5,519	7,055	9,949	13,633	14,660
March	-	6,850	8,938	11,492	15,154	16,084
April	2,170	7,148	8,057	9,478	11,498	15,355
May	4,404	6,754	7,409	10,400	13,363	---
June	6,070	6,696	8,737	10,956	13,915	---
July	6,907	7,175	8,757	8,518	12,032	---
August	6,567	6,332	8,532	10,484	14,853	---
September	6,938	7,561	7,577	8,471	13,514	---
October	7,474	7,439	8,165	9,842	12,662	---
November	5,029	5,960	7,848	11,243	14,145	---
December	6,510	7,604	8,614	11,050	14,546	---
Subtotal	**52,069**	**81,161**	**96,521**	**120,504**	**162,714**	**59,866**
Total Filings	***572,835***					

[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 are 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 April 30, 2001—

State/Territory	1996	1997	1998	1999	2000	2001
Alabama	362	445	406	528	689	323
Alaska	65	59	131	157	353	90
American Samoa	2	0	7	2	10	1
Arizona	1,905	3,104	2,392	2,505	3,894	1,190
Arkansas	206	335	297	430	560	194
California	12,631	18,143	22,836	24,995	43,304	16,401
Colorado	881	1,069	1,475	1,679	2,146	1,010
Connecticut	422	785	937	4,449	4,873	1,556
Delaware	1,136	1,429	1,657	2,004	3,670	1,498
District of Columbia	174	233	274	285	467	189
Federated States of Micronesia	1	3	3	1	3	0
Florida	4,195	6,560	6,988	7,913	9,918	3,346
Georgia	907	1,492	1,656	2,205	3,141	1,095
Guam	27	80	52	84	73	22
Hawaii	406	536	553	550	731	303
Idaho	109	150	120	186	402	127
Illinois	1,601	2,763	2,863	3,793	4,790	1,780
Indiana	596	764	955	1,163	1,349	465
Iowa	267	363	325	427	493	253
Kansas	275	287	362	555	520	214
Kentucky	271	388	424	751	853	349
Louisiana	500	594	666	902	1,943	674
Maine	120	186	189	213	241	117
Marshall Islands	0	0	0	2	0	1
Maryland	652	937	1,182	1,537	2,069	709
Massachusetts	885	1,402	1,828	2,477	2,747	1,073
Michigan	1,175	1,719	1,848	2,746	3,765	1,392
Minnesota	1,000	2,266	2,208	2,511	2,893	945
Mississippi	160	251	222	283	521	208
Missouri	638	966	1,139	1,215	1,590	686
Montana	71	107	100	152	220	75
Nebraska	194	249	315	371	615	277
Nevada	695	1,486	1,966	2,063	3,074	932
New Hampshire	273	506	416	573	448	104
New Jersey	949	1,530	2,377	3,349	4,197	910

Exhibit 2 (continued)

SAR Filings by States and Territories

—For the Period April 1, 1996 through April 30, 2001—

State/Territory	1996	1997	1998	1999	2000	2001
New Mexico	237	237	286	307	403	134
New York	5,511	9,661	13,297	17,748	19,138	7,023
North Carolina	939	1,621	2,063	2,366	2,978	911
North Dakota	43	215	212	122	224	58
Northern Mariana Islands	22	5	13	33	57	19
Ohio	975	1,722	2,198	2,295	3,319	1,347
Oklahoma	395	497	503	698	813	198
Oregon	602	1,117	1,196	1,807	2,471	752
Overseas	12	39	7	2	22	5
Pennsylvania	1,510	2,481	2,409	3,571	3,535	1,320
Puerto Rico	188	562	440	316	1,063	338
Rhode Island	166	290	283	503	495	146
South Carolina	312	563	627	668	733	342
South Dakota	326	430	547	675	267	146
Tennessee	569	799	890	993	1,555	627
Texas	4,001	4,913	6,158	7,605	10,119	3,883
U.S Virgin Islands	3	9	12	17	32	21
Unknown/Blank	318	205	28	26	249	34
Utah	387	882	1,068	1,361	2,219	910
Vermont	57	88	61	58	69	31
Virginia	634	1,208	1,501	1,535	2,001	802
Washington	771	1,733	2,176	3,124	3,362	1,208
West Virginia	114	154	161	154	182	54
Wisconsin	372	551	649	755	1,006	361
Wyoming	27	43	54	40	67	104
Total	**52,242**	**81,212**	**96,008**	**119,835**	**162,941**	**59,283**

Exhibit 3

Frequency Distribution of SAR Filings Ranked by States and Territories in Descending Order
—For the Period April 1, 1996 through April 30, 2001—

Rank	State/Territory	Filings (Overall)	Percentage[2] (Overall)
1	California	138,310	25.185%
2	New York	72,378	13.170%
3	Florida	38,920	7.080%
4	Texas	36,679	6.670%
5	Illinois	17,590	3.200%
6	Arizona	14,990	2.710%
7	Pennsylvania	14,826	2.700%
8	New Jersey	13,312	2.420%
9	Connecticut	13,022	2.370%
10	Michigan	12,645	2.300%
11	Washington	12,374	2.250%
12	Ohio	11,856	2.150%
13	Minnesota	11,823	2.150%
14	Delaware	11,394	2.070%
15	North Carolina	10,878	1.980%
16	Georgia	10,496	1.910%
17	Massachusetts	10,412	1.890%
18	Nevada	10,216	1.860%
19	Colorado	8,260	1.500%
20	Oregon	7,945	1.440%
21	Virginia	7,681	1.390%
22	Maryland	7,086	1.290%
23	Utah	6,827	1.240%
24	Missouri	6,234	1.130%
25	Tennessee	5,433	Less than 1%
26	Indiana	5,292	Less than 1%
27	Louisiana	5,279	Less than 1%
28	Wisconsin	3,694	Less than 1%
29	South Carolina	3,245	Less than 1%
30	Oklahoma	3,104	Less than 1%
31	Hawaii	3,079	Less than 1%
32	Kentucky	3,036	Less than 1%
33	Puerto Rico	2,907	Less than 1%
34	Alabama	2,753	Less than 1%

Exhibit 3 (continued)

Frequency Distribution of SAR Filings Ranked by States and Territories in Descending Order
—For the Period April 1, 1996 through April 30, 2001—

Rank	State/Territory	Filings (Overall)	Percentage[2] (Overall)
35	South Dakota	2,391	Less than 1%
36	New Hampshire	2,320	Less than 1%
37	Kansas	2,213	Less than 1%
38	Iowa	2,128	Less than 1%
39	Nebraska	2,021	Less than 1%
40	Arkansas	2,002	Less than 1%
41	Rhode Island	1,883	Less than 1%
42	Mississippi	1,645	Less than 1%
43	District of Columbia	1,622	Less than 1%
44	New Mexico	1,604	Less than 1%
45	Idaho	1,094	Less than 1%
46	Maine	1,066	Less than 1%
47	North Dakota	874	Less than 1%
48	Unknown/Blank	860	Less than 1%
49	Alaska	855	Less than 1%
50	West Virginia	819	Less than 1%
51	Montana	725	Less than 1%
52	Vermont	364	Less than 1%
53	Guam	338	Less than 1%
54	Wyoming	335	Less than 1%
55	Northern Mariana Islands	149	Less than 1%
56	U.S. Virgin Islands	94	Less than 1%
57	Overseas	87	Less than 1%
58	American Samoa	22	Less than 1%
59	Federated States of Micronesia	11	Less than 1%
60	Marshall Islands	3	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 April 30, 2001—

Rank	Violation Type	Filings (Overall)	Percentage[3] (Overall)
1	BSA/Structuring/Money Laundering	288,072	46.0%
2	Check Fraud	79,892	13.0%
3	Other	44,700	7.0%
4	Counterfeit Check	32,025	5.2%
5	Defalcation/Embezzlement	27,254	4.4%
6	Credit Card Fraud	26,361	4.3%
7	Check Kiting	23,946	3.9%
8	Unknown/Blank	23,379	3.8%
9	Mortgage Loan Fraud	13,202	2.1%
10	Consumer Loan Fraud	12,792	2.1%
11	False Statement	12,295	2.0%
12	Mysterious Disappearance	9,643	1.6%
13	Misuse of Position or Self Dealing	9,109	1.5%
14	Commercial Loan Fraud	5,241	Less than 1%
15	Debit Card Fraud	3,885	Less than 1%
16	Wire Transfer Fraud	3,614	Less than 1%
17	Counterfeit Credit/Debit Card	2,353	Less than 1%
18	Counterfeit Instrument (Other)	1,741	Less than 1%
19	Bribery/Gratuity	606	Less than 1%
20	Computer Intrusion[4]	127	Less than 1%

[3] All percentages are approximate.

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

Exhibit 5

Frequency Distribution of SAR Filings by Characterization of Suspicious Activity —For the Period April 1, 1996 through April 30, 2001—

Violation Type	1996	1997	1998	1999	2000	2001
BSA/Structuring/Money Laundering	21,655	35,625	47,223	60,983	90,606	31,980
Bribery/Gratuity	94	109	92	101	150	60
Check Fraud	9,078	13,245	13,767	16,232	19,637	7,933
Check Kiting	2,902	4,294	4,032	4,058	6,163	2,497
Commercial Loan Fraud	583	960	905	1,080	1,320	393
Computer Intrusion	0	0	0	0	65[5]	62
Consumer Loan Fraud	1,190	2,048	2,183	2,548	3,432	1,391
Counterfeit Check	2,405	4,226	5,897	7,392	9,033	3,072
Counterfeit Credit/Debit Card	391	387	182	351	664	378
Counterfeit Instrument (Other)	219	294	263	320	474	171
Credit Card Fraud	3,340	5,075	4,377	4,936	6,275	2,358
Debit Card Fraud	261	612	565	721	1,210	516
Defalcation/Embezzlement	3,286	5,284	5,252	5,178	6,117	2,137
False Statement	1,880	2,200	1,970	2,376	3,051	818
Misuse of Position or Self Dealing	952	1,532	1,640	2,064	2,186	735
Mortgage Loan Fraud	1,318	1,720	2,269	2,934	3,515	1,446
Mysterious Disappearance	1,216	1,765	1,855	1,854	2,225	728
Wire Transfer Fraud	302	509	593	771	972	467
Other	4,836	6,675	8,583	8,739	11,148	4,719
Unknown/Blank	1,539	2,317	2,691	6,961	6,971	2,900

For statistical information on the Characterization of Suspicious Activity by States/Territories by Year see Appendix 1.

[5] Separate box for this violation was added to form TD F 90-22.47 in June 2000. Statistics date from that period.

Exhibit 6

SAR Filings by Primary Federal Regulator[6]
—For the Period April 1, 1996 through April 30, 2001—

Regulator	Total Filings by Year					
	1996	1997	1998	1999	2000	2001
Federal Reserve Board	5,875	9,581	10,800	14,656	18,269	7,068
Federal Deposit Insurance Corporation	10,339	14,909	14,735	15,883	20,089	7,819
Office of the Comptroller of the Currency	26,298	41,425	51,556	64,945	93,443	34,223
Office of Thrift Supervision	6,014	9,122	11,375	12,316	15,982	5,366
National Credit Union Administration	2,141	2,631	2,846	3,041	3,674	1,618
Unspecified	1,402	3,529	5,209	9,663	11,257	3,772

[6] Unspecified regulator indicates that the SAR form was filed by a non-bank financial institution that is not directly supervised by one of the five agencies listed above. Such entities that 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 broker/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 April 30, 2001—

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 recording a count for each agency to which a direct referral was 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	2001	Total
Federal Law Enforcement							
Federal Bureau of Investigation	2,355	3,833	4,174	4,779	3,386	280	18,807
Internal Revenue Service	1,138	2,687	2,183	2,118	1,083	258	9,467
U.S. Secret Service	894	1,609	1,223	1,060	746	75	5,607
Postal Inspection Service	340	610	636	644	728	170	3,128
U.S. Attorney's Office	185	132	84	106	101	42	650
U.S. Customs Service	52	62	101	83	66	4	368
Department of Treasury	55	56	30	43	23	7	214
Drug Enforcement Administration	11	18	23	8	127	7	194
Naval Criminal Investigative Service/ United States Navy	14	18	6	17	13	8	76
Department of Justice	9	4	10	8	10	20	61
Social Security Administration (IG)	4	9	11	8	9	10	51
Immigration & Naturalization Service	0	3	12	6	11	0	32
Sub-Total	5,057	9,041	8,493	8,880	6,303	881	38,655
Other Federal Law Enforcement	28	63	83	80	72	48	374
Total Federal Law Enforcement	5,085	9,104	8,576	8,960	6,375	929	39,029
Regulatory							
Federal Deposit Insurance Corporation	24	26	25	22	42	28	167
Federal Reserve Board	46	29	27	13	15	106	236
Office of the Comptroller of the Currency	17	21	19	24	37	17	135

Exhibit 7 (continued)

Direct Referrals of SARs by Financial Institutions to Law Enforcement[7] and Regulatory Agencies
—For the Period April 1, 1996 through April 30, 2001—

Agencies	1996	1997	1998	1999	2000	2001	Total
Regulatory (continued)							
Securities & Exchange Commission	15	11	21	8	44	8	107
Office of Thrift Supervision	7	3	3	6	0	5	24
National Credit Union Administration	4	5	1	4	2	5	21
Federal Trade Commission	0	0	0	7	2	1	10
National Association of Securities Dealers	0	1	1	1	1	0	4
Total Regulatory	**113**	**96**	**97**	**85**	**143**	**170**	**704**
State & Local Law Enforcement							
City/Local Police Department	4,407	6,978	7,588	7,994	8,586	3,523	39,076
County/Parish	789	1,235	938	1,253	1,533	707	6,455
D/A, A/G, or Prosecutor's Office[8]	317	445	347	401	373	230	2,113
State Police	181	295	263	289	329	117	1,474
Other State and Local	89	106	107	135	129	248	814
Total State & Local Law Enforcement	**5,783**	**9,059**	**9,243**	**10,072**	**10,950**	**4,825**	**49,932**
Other							
Pending	8	56	40	50	31	3	188
Unspecified	254	184	164	234	351	112	1,299
Private Industry[9]	29	27	33	12	15	12	128
Foreign Law Enforcement[10]	51	74	69	86	59	19	358
FinCEN/DCC	45	224	153	131	186	63	802
GRAND TOTAL	***11,368***	*18,824*	***18,375***	***19,630***	***18,110***	***6,133***	***92,440***

[7] Some SARs may reference making referrals to multiple law enforcement agencies.
[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. The value of this information is that financial institutions have reported these suspicious activities and other financial institutions should be alert to similar suspicious activities occurring in their institutions. 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* — Computer Intrusion — was suggested as a topic for discussion by the financial industry since it was added as a new characterization of suspicious activity on the revised SAR form dated June 2000. Law enforcement identified the need for this category as a result of reports from financial institutions regarding possible attempts to intrude into their computer systems.

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

- remove, steal, procure or otherwise affect funds of the institution or the institution's customers;
- remove, steal, procure or otherwise affect critical information of the institution including customer account information; or
- damage, disable or otherwise affect critical systems of the institution.

For purposes of this reporting requirement, computer intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial data or other critical information.

During the first year that computer intrusion was added to the SAR form (June 1, 2000 – May 31, 2001), 147 SARs were filed by financial institutions in 34 states and Puerto Rico identifying computer intrusion as a violation. All of the SARs were filed by depository institutions with those in New York, California and Illinois accounting for nearly 30 percent. In addition to the computer intrusion violation, almost 10 percent of the SAR narratives described instances of identity

fraud as a vehicle for establishing new accounts via the Internet. The reporting financial institutions referred 55 of those suspicious activities to law enforcement; 32 of them were referred to the FBI.

Of the 147 SARs that identified computer intrusion as a violation in Part III, block 35, of the SAR, 64 SAR narratives described computer-related activity that did not meet the criteria for computer intrusion. For example, many SAR narratives described instances of individuals hacking into computer systems and changing the content on web pages, but not accessing sensitive bank or customer information systems. These activities should not be reported as computer intrusion for purposes of SAR reporting. See Section 5 under Special SAR Form Completion Guidance Related to Computer Intrusion for guidance.

Of the 147 SARs filed, 83 narratives described activities that were considered computer intrusion as SAR reportable activity. Of those 83 SARs, more than 60% described activity in which the computer intrusion involved a bank employee. In these instances, the bank employee utilized his/her position and breakdowns in internal controls to embezzle or defraud the bank.

Two SAR narratives described attempted intrusions through a worm or virus, while other SAR narratives described unsuccessful attempts to intrude into the system and then send bulk email/spam in order to overwhelm and disable the system. Two SAR narratives described failed attempts to intrude into the bank's critical information systems. In those instances, "intrusion detection systems" were running on those banks' servers, foiling intrusion attempts.

One SAR narrative described an instance where an unknown entity registered a new domain name and created a website that was similar to one being utilized by a credit union. This phony website deceived credit union members, resulting in the victims entering their home banking security information, thus allowing the perpetrator unauthorized access to their accounts via the Internet.

Another SAR narrative described a similar situation, where the suspect overrode web protocols and created a near-duplicate but sham bank website. Customers of the legitimate bank were unaware that information entered on the sham web page never made it to the bank. The legitimate bank that caught and reported the scam on a SAR did not know if any financial information was captured by the sham bank's website and used to conduct illicit activity.

While not an instance of computer intrusion, one particular scheme is worth noting. A Russian individual attempted to hack into at least four banks during the period of late April/early May 2001. He contacted the banks to notify them that he was successful in his attempt to intrude into their systems and identified several vulnerabilities that allowed access to all logs, files, and passwords. At

that point, he attempted to extort bank officials by claiming that he would assist them with correcting their computer system vulnerabilities.

Four SARs described a bill paying service whose customer information appeared to be compromised by someone within the organization. The intruder obtained valid ID and PIN numbers of customers and then initiated unauthorized automated clearinghouse debits from various accounts.

During the review of these SARs, it was discovered that some financial institutions were not certain when a SAR should be filed. When a suspicious activity occurs, an institution should file a SAR within 30 days if the suspect is identified or within 60 days if the individual(s) cannot be identified. Some of the narratives stated that the filing institution was waiting until a particular monetary threshold was met prior to filing the SAR. Although banks are required to file a SAR when the suspicious activity amounts to $5,000 or more, banks are permitted to file at a lower dollar threshold.

Of the 147 SARs filed on computer intrusion, 17 (almost 12%) did not complete Part V (the narrative). In a few instances, the narrative indicated that documents were attached to the form. As the SAR form instructions indicate, "this section of the report is critical. … Supporting documentation such as spreadsheets, photocopies of canceled checks or other documents, surveillance photos, etc., must be retained at the financial institution. Indicate in Part V what documentation is being retained."

2. Other Notable Trends

SAR Filings Demonstrate Use of Money Transmitters as Money Laundering Vehicle

The vast majority of companies in the United States that make up the money services businesses (MSB) industry recognize that the products and services they provide may be vulnerable to abuse. As reported in the Industry Forum section of the June Issue of the *SAR Activity Review*, some of the national MSBs, including the leading money transmission services, money order and traveler's checks issuers, check cashing businesses and currency exchange providers have developed internal systems to detect suspicious activity.

Since the inception of the SAR reporting requirements in April 1996, MSBs have *voluntarily* filed more than 14,000 reports of suspicious activity and they have taken other steps to prevent and detect possible money laundering activity, including imposing customer identification requirements at thresholds below current regulatory requirements and closing sales locations where appropriate. In

addition, SARs have been filed by banks on financial activity associated with licensed and unlicensed MSBs every year. The factual situations outlined below are provided as examples of scenarios that have been reported as suspicious by money transmitters . The next issue of the *SAR Activity Review* will focus on and summarize the reports of suspicious activities filed by depository institutions.

Overview: SARs filed by money transmitter companies, both primary companies (companies that own a money transmitter business) and agent businesses (companies that act as agents), indicate that there are many varied patterns of suspicious activity involving money transmitter companies. Primary among those are customer attempts to disperse transactions and circumvent record keeping dollar amount thresholds. Reports of suspicious activity include:

- transactions structured in dollar amounts below record keeping requirement thresholds;
- multiple customers (senders and/or receivers) sharing common identifiers (last names, street addresses, telephone numbers);
- single send customers using multiple addresses;
- successive funds transfers being sent (often a few minutes apart) in the same dollar amounts structured under record keeping thresholds;
- transactions conducted by a group or cluster of groups of customers;
- single send customer going to different agent business locations in a limited time period (e.g., one afternoon); and
- occupations listed for customers that would not seem to justify the level of financial activity.

SARs Filed by Money Transmitters: Money transmitter companies are voluntarily filing SARs on customer transactions attempted, initiated or concluded at agent business locations (e.g., grocery store; liquor store; gas station). These filings reveal many varied and complex patterns of activity that appear to involve customers dispersing their transactions and/or structuring dollar amounts of the funds transfers in an attempt to avoid the dollar threshold for required record keeping.[11] While there are many variations of the reported suspicious activities, the following patterns are intended to serve as representative samples.

---

[11] Transactions may be structured, for example, to avoid the BSA funds transfer record keeping rules for transactions $3,000 and above. They may also be structured to avoid company practices requiring customer photo identification on transactions $1,000 or above, or to avoid the currency transaction report requirements for transactions of more than $10,000.

The primary methods by which the customers of money transmitters appear to disperse and structure transactions to avoid the record keeping requirement thresholds (e.g., below $3,000 or in some instances thresholds of $1,000 imposed by policies of primary money transmitter companies) fit within a combination of the categories listed below:

- multiple send customers send funds transfers to the same receiver or multiple receivers;
- a single send customer sends multiple funds transfers to the same receiver or multiple receivers;
- transactions involving successive funds transfers (often sent a few minutes apart);
- transfers being sent in same dollar amounts structured below record keeping requirements;
- multiple senders and/or receivers sharing common identifiers (e.g., last names, street addresses, telephone numbers--sometimes with slight variations);
- transactions that involve multiple send customers often appear to be conducted, at least on the sending side, at the same agent business office;
- transactions involving multiple send customers in a suspicious group or a cluster of groups (discussed further below);
- transactions involving a single send customer going to different send agent business locations (discussed further below);
- a single send customer using more than one address and/or suspected false address(es).

Example of Basic Structuring Attempt:

One pattern involves obvious attempts by a customer(s) to structure transactions below the record keeping/reporting thresholds. In one example, a customer had sent 11 money transfers (totaling $103,000) to 10 receivers in Nigeria. Two days later, the same customer attempted to send $157,000 (in 18 transactions structured under the CTR threshold) to multiple receivers in Nigeria. After the primary money transmitter company refused the transactions and explained recording/reporting requirements and pay out restrictions to the customer, the customer

then attempted to send eight individuals (his employees) to the same agent business location to send funds to Nigeria on his behalf. These transactions were also refused by the primary company.

Example of Suspicious Activity on the Receive Side:

Suspicious activity has been reported on the receive side of the funds transfer. One money transmitter reported that a receive customer collected numerous funds transfers in a total amount of approximately $66,000 from 36 senders, over a two-month period. The receive customer listed two different addresses as his primary residences and typically collected multiple transfers on the same day, but picked up the funds transfers at different agent business locations. The transfers were usually sent in structured amounts. The reporting money transmitter company cited the number of senders, structured dollar amounts, and use of different permanent addresses by the receive customer as contributing to the suspicious character of the activity.

Example of a Single Customer Going to Multiple Agent Business Locations:

One suspect customer in one afternoon went to several different U.S.-based agent business locations (of the same money transmitter). At different agent locations, that customer initiated successive, multiple funds transfers in amounts below the record keeping threshold to several receive customers (or sometimes a single receive customer) located either domestically or abroad.[12]

Example of a group or a "cluster" of groups sending successive and structured funds transfers:

There are many patterns of suspicious activity that involve a group of suspect customers or a cluster of groups. These patterns involved:

- multiple customers operating in a group, or even within a cluster of groups, initiate multiple and successive funds transfers;
- the funds transfers in the same (or close) dollar amounts structured below the record keeping rule threshold;

[12] Many SARs portraying this pattern identified Nigeria, Panama, Jamaica, Mexico, Suriname, Costa Rica, Israel, Netherlands, Dominican Republic, Ecuador, and Ghana as locations for the receivers of the money transfers. Nicaragua, Russia, South Africa, Singapore, Senegal, and Spain were identified in single instances as locations of the money transfer receivers.

- the customers in a group, and/or within a cluster of different groups, share some common identifiers (last names or street addresses, sometimes with slight variations);
- a cluster of groups using the same send agent business;
- the same named individual and/or common street names/addresses appear (i.e., "float around") repeatedly within different groups of a given cluster; and
- customers operating within a cluster of groups repeatedly appear with different addresses.

The following is an example that involves a group of customers entering the same send agent business location and initiating successive funds transfers in the same structured amount to the same receiver in Nigeria, where the government imposes a $10,000 per person per day limit on funds tranfers[13]:

Suspect A sends $2,500 at 1:44 p.m.;
Suspect B sends $2,500 at 1:47 p.m.;
Suspect C sends $2,500 at 2:06 p.m.;
Suspect D sends $2,500 at 2:11 p.m.;
Suspect E sends $2,500 at 2:19 p.m.; and
Suspect F (same last name as receiver) sends $2,500 at 2:22 p.m.

About two weeks later, another group of six customers entered the same agent business location as above and conducted an identical pattern of successive (a few minutes apart) and structured dollar amount transactions also to Nigeria. Some of the individuals in this later group had the same last names as the customers in the first group (in addition to some slight last name variations). Additional SARs filed by the primary company identified several other groups of customers initiating money transfers at this same agent business location, in the same manner, and within the same overall time frame.

SARs Filed by Primary Company on Suspicious Activity at Agent Businesses

As a result of some primary money transmitter companies' monitoring mechanisms, SARs have been filed on suspicious activity conducted at agent business

---

[13] Besides Nigeria, international transfers sent in this manner have also been destined to Jamaica, Colombia, Mexico, Netherlands, El Salvador, Dominican Republic, Ukraine, Kenya, Bahamas, Ecuador, Palestine, Albania, Spain, India, Costa Rica, Russia, Guatemala, Nicaragua, South Africa, Trinidad, Antigua, Thailand, Argentina. Single instances have been observed for Qatar, Hungary, Georgia, Slovakia, Poland, and Panama (based upon those SARs examined in this representative study).

locations. One primary money transmitter company, for example, reported terminating its relationship with one of its agent businesses after the agent business appeared to be circumventing the primary company's own internal record keeping and reporting requirements. The agent business had initiated 610 money transfers to Colombia for various customers during a three-month period, of which nearly 85% were in amounts below the primary company's record keeping and reporting threshold.

Another primary money transmitter company indefinitely suspended a particular agent business after the primary company detected unusual send and receive customer patterns at the agent business location. In that SAR, it was reported that over a six-month monitoring period, the values of funds transfers initiated at the particular agent business were at consistently high levels. For example, send transactions occurring through the agent business location involved 15 different senders, totaling $1.5 million. Total dollar amounts for the entire six-month period sent by each individual ranged from $5,000 to approximately $366,000. Total dollar amount for the entire six-month period received by each individual ranged from $5,700 to approximately $51,200. Other factors not disclosed in the filed report contributed to the suspicious nature of the activity.

Use of Traveler's Checks to Disguise Identities

SAR reporting indicates that criminals may be using traveler's checks as a money laundering tool to provide anonymity to the purchaser and/or the ultimate payee. Although traveler's checks may be a preferred instrument for conducting large business transactions in some countries, the use of traveler's checks to negotiate these transactions may offer the opportunity to commingle illicit funds with legitimate funds. Several major U.S. banks and traveler's check issuers have detected and reported suspicious practices involving the use of hundreds of thousands of dollars in traveler's checks per instance, often in strings of sequentially numbered thousand-dollar traveler's checks. In some cases, the payee was a numbered account in a foreign bank. Frequently, the name and/or address on the purchase agreement were:

- left blank;
- unverifiable;
- illegible; or
- not matching the signature name on the corresponding traveler's checks.

Mexico, Nigeria, Israel, and a number of East Asian countries have been cited in multiple SARs as the point of origin or negotiation for instruments involved in this type of activity. An example was the purchase of traveler's checks from an investment house/travel agency in Asia, where the traveler's check seller appeared to have

gone to unusual lengths to conceal the identity of the buyers. One employee of the traveler's check seller personally signed the purchase agreements for $27 million worth of traveler's checks. When the traveler's check issuer told the seller to have the buyer sign the purchase agreement, the traveler's check seller started producing purchase agreements with many different names, but frequent similarities in handwriting.

Reports of Solicitation Letters (Advanced Fee Fraud or 4-1-9 Scams)

SARs increasingly reference bank account solicitation letters coming from suspect individuals in Nigeria, South Africa, or Ghana representing themselves to be former or current high-level government officials, soldiers or influential professionals (or their spouses). The letters are typically directed at bank officials and/or specific customers (individuals or businesses) of banks, and request direct access to bank account and other identification information to arrange for a supposed large transfer of funds (typically tens of millions of dollars) from Nigeria, South Africa, or Ghana into the subject account. This type of advanced fee fraud is called a "419 scam,"[14] but is often reported in SARs in the *BSA/Structuring/Money Laundering* category, since the letters usually seem to be soliciting assistance for clandestine currency flight. The large sums of funds available are often described as resulting from over-invoicing or paybacks on contracts (e.g., petroleum; oil; equipment supply; construction). Some Ghanaian letters claim to have money embezzled from the UNITA rebels in Angola in two trunks in Accra, Ghana. The requester may also typically indicate that they are not allowed to own or operate foreign accounts, since they are officials of the Nigerian or South African government, or expatriates from Angola or Sierra Leone. A substantial percentage fee (e.g., 20-30%) for the use of the account is typically offered to the recipient of the correspondence. In one example, the letter stated that the "source of the funds are drug free and 100% risk free…."

The U.S. Department of State, Bureau of International Narcotics and Law Enforcement Affairs published an April 1997 report entitled *Nigerian Advance Fee Fraud* that provides examples of the various business schemes used by Nigerian criminals to fraudulently obtain funds from U.S. businesses. This report can be found at www.http://travel.state.gov. Individuals receiving a suspicious business proposal from Nigerian or other African sources should contact the U.S. Secret Service, Financial Crimes Division, 1800 G Street, N.W., Room 942, Washington, D.C. 20233. The phone number is (202) 435-5850, fax number is (202) 435-5031. Nigerian Advance Fee Fraud letters can be emailed to the Secret Service at 419.fcd@usss.treas.gov.

---

[14] The "419" refers to the section of the Nigerian penal law that deals with advanced fee fraud. The 419 penal law was revised and expanded with the issuance in April 1995, of Presidential Decree No. 13 entitled *Advance Fee Fraud and other Fraud Offenses Decree 1995.*

Update on Identity Theft

In the June 2001 Issue of the *SAR Activity Review*, Identity Theft was selected as the Highlighted Trend based on the financial industry's perception of increases in both the incidence of identity theft-based fraud and increased SAR reporting. Identity theft and related fraudulent activities have been reported by financial institutions since SAR reporting began in 1996. Results of FinCEN's analysis of SAR data confirmed that there had been an increase in the incidence of identity theft and increased SAR reporting. Details of the SAR narratives describing examples of identity theft were provided in the June 2001 *SAR Activity Review*.

Since December 1, 2000, financial institutions have filed 352 SARs relating to identity theft. That amounts to a 50 percent increase from the same period a year ago. The number of SARs filed each year relating to identity theft is shown in the table below:

	1996*	1997	1998	1999	2000	2001**
Number of SARs	21	44	81	267	637	332

* Partial year- April 1, 1996 - December 31, 1996
** Partial year- January 1, 2001 - April 30, 2001

There have been a total of 236 financial institutions that reported incidents of identity theft since the beginning of SAR reporting requirements. However, 42 financial institutions that had not previously reported instances of identity theft reported such activity since January 1, 2001. Identity theft was reported by financial institutions located in 43 states and the District of Columbia. Financial institutions in California and North Carolina each account for about 15 percent of the number of SARs filed describing identity theft or related frauds. Since December 1, 2000, financial institutions referred 81 SARs to law enforcement.

Because the rate of identity theft incidents continues to increase, the following information is provided to assist in reporting identity theft:

The Federal Trade Commission has developed a pamphlet to assist consumers in avoiding identity theft and, in instances of abuse, to give steps to take in addressing stolen identities. The pamphlet can be obtained from the FTC's website at www.consumer.gov/identitytheft. Another resource on identity theft can be found at www.consumer.gov/knowfraud. In addition, federal bank supervisors recently released guidance to banking organizations on identity theft and pretext calling. The guidance can be found on their respective 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 guidance related to identity theft and pretext calling.

3. Other SAR Analysis Issues

Percentage of SARs Reporting Structuring

Field 35 of the SAR form—Summary Characterization of Suspicious Activity—does not break out BSA, Structuring or Money Laundering violations into separate check-off categories. As a result, it has been difficult to provide accurate estimates of the levels of the different types of suspicious activity reported under the catch-all BSA/Structuring/Money Laundering characterization. In particular, questions are frequently raised by both law enforcement and the financial industry concerning the percentage of SARs filed that involve structuring.

To better respond to these questions, FinCEN conducted an analysis of the national SAR database involving the extraction of a random set of 2,500 SARs for each year from 1996 to 2001. The subset of SARs in which the BSA/Structuring/Money Laundering box was checked was then extracted. The narratives of these SARs were then analyzed to determine if structuring activity formed the basis for the report. The resulting set of SARs—those involving structuring—was used to establish sample percentages for structuring for each year. These samples can be extrapolated into estimates of the overall percentage of SARs reporting structuring. Results of this analysis are shown in the following table:

Percentage of SARs Reporting Structuring

Year	Total SARs	BSA/ML SARs	Random Sample	Sample BSA/ML/ Structuring Count	Structuring as % of Sample	Estimated Structuring SARs as % of Total
1996*	50,920	21,549	2,500	1,473	58.9	24.9
1997	79,076	35,646	2,500	1,360	54.4	24.5
1998	94,385	47,072	2,500	1,408	56.3	28.1
1999	120,424	61,896	2,500	1,450	58.0	29.8
2000	150,289	84,166	2,500	1,565	62.6	35.1
2001**	51,283	27,951	2,500	1,618	64.7	35.3

* Partial year, April through December
** Partial year, January through mid-May

Voluntary SAR Filings

A small part of the total volume of SARs filed relates to reports filed voluntarily by brokers and dealers in securities who are not affiliated with banks; money services businesses; or gaming businesses that have no regulatory requirements at this time that mandate SAR filings. For the June 2001 Issue of the *SAR Activity Review*, at the request of the filing industries, FinCEN conducted a study to determine the number of SARs being filed voluntarily. The following table provides an update of findings relevant to voluntary SAR filings from April 1996 through April 2001.

Industry	Number of SARs	Referred to Law Enforcement	Violation Type (percentage)
Casino SAR[15]	59	6	BSA/Structuring/ML - 51.75% Other - 46.55%
Casino SARC[16]	1,169	156	Structuring - 32% Large Transactions w/Minimal Gaming – 16.5% Money Laundering – 12.15%
Credit Card & Phone Card Service	302	100	Credit Card Fraud – 61.6% Debit Card Fraud – 14.5%
Insurance	126	5	BSA/Structuring/ML – 64.25% Other – 35%
Mortgage	220	40	Mortgage Loan Fraud – 95.6%
MSB	14,398	3,098	BSA/Structuring/ML – 98%
Realty/Real Estate Management	6	4	BSA/Structuring/ML – 100%
Securities, Investment, Brokerage Service	1,930	133	BSA/Structuring/ML – 71% Check Fraud – 10.3%
Travel Servicess	67	65	BSA/Structuring/ML - 94%
Miscellaneous	8	3	Other - 37.7% False Statement - 16.6%
Total	**18,285**	**3,610**	**BSA/Structuring/ML[17] - 91.25%**

[15] Casinos that filed reports of suspicious activity on the bank SAR form.

[16] Casinos located outside of Nevada (which has mandatory SAR requirements) and casinos located in New Jersey that filed SARCs prior to their October 12, 2000 mandatory SAR requirements went into effect. For the Casino Suspicious Activity Reports the reporting period is late 1997 through April 2001.

[17] BSA/Structuring/ML percentage average does not contain violation(s) as reported on SARCs for same period.

Section 3
Issues with International Impact

Non-Cooperative Countries and Territories

In June 2001, *FinCEN Advisories* were issued notifying financial institutions that previous *FinCEN Advisories* on the Bahamas, the Cayman Islands, Liechtenstein and Panama calling for enhanced scrutiny to financial transactions originating in, or routed through, those jurisdictions were being withdrawn. This action followed the June 22, 2001 publication of the Financial Action Task Force on Money Laundering's (FATF) 12th annual report[18] and the decision to remove the Bahamas, the Cayman Islands, Liechtenstein and Panama from the FATF list of "non-cooperative countries and territories" (NCCTs) in the global fight against money laundering.[19] At the same time, the FATF identified serious deficiencies in the anti-money laundering regimes in Egypt, Guatemala, Hungary, Indonesia, Myanmar and Nigeria, and added them to the list of NCCTs.

On September 7, 2001, FATF announced the results of its discussions on "non-cooperative" jurisdictions since the publication of its second report on the non-cooperative countries and territories (NCCTs) dated June 2001.[20] During that period, FATF reviewed the status of legislative efforts by the Governments of Russia, Nauru and the Philippines, which had been notified in June that failure to enact significant anti-money laundering legislation by September 30, 2001 would result in the imposition of countermeasures by FATF members.

Also, upon review of several jurisdictions, the FATF added two more countries – Grenada and Ukraine—to its NCCT list because the countries were found to have serious deficiencies in their anti-money laundering regimes. The updated list of NCCTs is as follows: Cook Islands, Dominica, Egypt, Grenada, Guatemala, Hungary, Indonesia, Israel, Lebanon, Marshall Islands, Myanmar, Nauru, Nigeria, Niue, Philippines, Russia, St. Kitts and Nevis, St. Vincent and the Grenadines, and Ukraine.

---

[18] See http://www.oecd.org/fatf/pdf/AR2001_en.pdf

[19] In addition, in August 2001, the FinCEN Advisory relating to Antigua and Barbuda was withdrawn.

[20] See http://www.oecd.org/fatf/pdf/NCCT2001_en.pdf

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 activity. Each issue of the *SAR Activity Review* includes new examples based on information received from law enforcement.

Federal Law Enforcement Use of SAR Data

SAR Leads to Former Deputy Sheriff Sentenced for Extortion and Title 31 Violations

A former California deputy sheriff pled guilty to extortion and Title 31 charges. He was sentenced to serve 60 months in prison followed by 5 years probation, and ordered to pay $300,000 in restitution to one of the victims. His wife received three years probation for related charges. The sentencings were the culmination of a joint investigation by Internal Revenue Service Criminal Investigation (IRS-CI) and a local police department. The subject, a martial arts expert, claimed that he was a former Green Beret and that he had Mafia connections. He used threats of violence and blackmail to extort as much as $1.3 million from various individuals. On one occasion, the subject used a Samurai sword and threatened to cut off a victim's fingers if he did not sign a promissory note payable to an individual described by the subject as a "Godfather type".

IRS-CI became aware of the illegal activity following the filing of a Suspicious Activity Report (SAR) by a local bank. The bank filed the SAR based on several factors including:

- the detection of a pattern of withdrawals inconsistent with the subject's normal business activity;
- conversations between the subject, and/or his wife with various bank tellers about large transactions that were inconsistent; and
- apparent attempts by the subject to structure deposits to avoid reporting requirements.

It was later discovered that the subject had opened the account using his mother-in-law's Social Security Number, and that he used several different identities. *(Source: IRS/Criminal Investigation)*

SAR Reveals Bank Fraud and Money Laundering Violations by RV Dealer

An Alaska motor home dealer was sentenced to 36 months in prison and 5 years probation after being found guilty of bank fraud and money laundering charges. The dealer was also ordered to pay restitution to the bank.

The motor home dealer obtained loans using trade-in motor homes as collateral. The dealer would then sell the used motor homes to individuals and fail to notify or repay the bank. The dealer defrauded the bank of approximately $500,000. Purchasers of the motor homes and RVs were told they would be mailed the title, which never happened because the banks held them.

The scheme was uncovered during an audit when the bank discovered that numerous motor homes pledged as collateral were no longer in the possession of the dealer. The bank filed a SAR detailing the fraud. The joint FBI and IRS-CI criminal investigation was initiated based on that SAR filing. During the investigation, approximately $600,000 was seized from the dealer, including over $490,000 in currency seized from a home safe. *(Source: IRS/Criminal Investigation)*

SAR Filings Lead to Discovery of Major Investment Scam

SARs filed by banks on an officer of an Indiana financial services company led to the discovery and dismantling of a scam that defrauded investors out of an estimated $35-40 million. The SARs were filed after the banks detected the officer was structuring cash withdrawals to avoid Currency Transaction Report (CTR) reporting requirements. Based on the information contained on the SARs, the IRS-CI and FBI initiated a joint investigation.

The investment company took in over $60 million from unsuspecting investors. Most of the funds were not invested, but were diverted to officers of the financial services company for their personal use. Many of the victims were elderly and lost much of their savings.

A vice president of the financial services company, who was involved in the scheme, entered into a plea agreement in which he admitted committing mail

fraud and money laundering violations. He was sentenced to 71 months in prison. Four additional individuals were also indicted on mail fraud and money laundering charges and are awaiting sentencing or trial. *(Source: IRS/Criminal Investigation)*

SAR Reveals Major Sports Betting Ring

Numerous individuals involved in a major Ohio sports betting ring have pled guilty to tax and gambling related charges. The ring came to light after a bank filed a SAR on a well-known professional athlete. The SAR was filed after the athlete used a $25,000 personal check to purchase ten $2,500 money orders. The next day, a different individual cashed the money orders in amounts under $10,000 at four different branches of the bank. Based on the information contained in the SAR, an IRS-CI investigation was initiated.

During the course of the investigation, it was learned that the professional athlete lost approximately $360,000 to the betting ring over a three-year period. The athlete was just one of many clients of the betting ring. On one New Year's weekend, one of the participants of the ring received over 400 phone calls at his residence, the bulk of which are believed to have involved sports betting activity. None of the participants in the ring reported the income from the ring on their personal tax returns. *(Source: IRS/Criminal Investigation)*

SAR Filings Reveal Methamphetemine Production Ring

The owner of a company that distributed various products to small independent convenience and grocery stores was sentenced to 188 months in prison after his conviction on drug, money laundering, and Title 31 charges. The company was distributing pallet-load quantities of psuedoephedrine to a broker who was reselling the drug to large-scale methamphetemine manufacturing operations. Psuedoephedrine is a common decongestant found in over-the-counter medications and a key ingredient in the manufacture of methamphetemine.

This joint IRS-CI and DEA investigation was initiated after the receipt of several SARs. One SAR outlined apparent attempts by the subject to structure currency deposits into his business bank account. In this case, the bank noted the company's pattern of daily $9,800 currency deposits. A second SAR was filed when the bank noted a shift in the company's deposit pattern. Instead of numerous currency deposits, the bank noticed the company began to deposit quantities of cashiers checks in amounts under $10,000.

Further investigation revealed that the small company sold about 9,000 cases of psuedoephedrine worth in excess of $5.6 million. This is enough to produce over

9,000 pounds of methamphetemine with a wholesale value of over $54 million. Eleven individuals were convicted and more than $4 million in cash and property was seized. *(Source: IRS/Criminal Investigation)*

SAR Filing Trips up Card Thief

A Pennsylvania man was sentenced to 15 months in prison followed by 3 years probation for structuring bank transactions to prevent the IRS from learning about profits earned from his role in sports card theft. The man owned a company involved in the sale of sports cards and was found to be stealing cards from a card manufacturer and selling them on the Internet. It is estimated that the subject sold between $350,000 and $500,000 in stolen cards. The scheme was uncovered when his bank filed a SAR after detecting apparent attempts by the subject to structure the cashing of third party checks to avoid reporting requirements. An IRS-CI investigation ensued, during which the theft scheme was uncovered. The subject pled guilty to tax and Title 31 charges. *(Source: IRS/Criminal Investigation)*

SAR Leads to Break-up of Stolen Check Ring

An individual walked into a Pennsylvania bank and opened one individual account and two business accounts. The individual then walked across the street to a different bank and opened three additional accounts. Unbeknownst to the individual, these two banks were in the process of merging and his behavior caught the attention of the bank security officer. The accounts were monitored and a SAR was filed when another subject attempted to negotiate a large third party check and the bank discovered that the address used to open the accounts was fictitious.

IRS-CI initiated an investigation based on this SAR. During the course of the investigation, it was discovered that these individuals were part of a ring that was stealing checks, written on U.S. banks, out of the mail in a foreign country and sending the checks to the United States to be negotiated. It was also discovered that the ring had opened up similar accounts at numerous other banks. Eleven individuals were identified as participants in the ring and they conducted over $1 million dollars in transactions at various banks. All were indicted on money laundering charges and seven have been convicted and sentenced to prison sentences. Four of the individuals involved are fugitives and believed to be out of the country. *(Source: IRS/Criminal Investigation)*

SAR Leads to Convictions of Members of Computer Chip Theft Ring

A New Hampshire bank filed a SAR on a group of individuals who were cashing numerous checks from a local salvage company for amounts under $10,000. Based on this SAR, an investigation was initiated by IRS-CI. During the course of the investigation, it was discovered that the men cashing the checks were working with an individual who was stealing computer memory chips from his employer, a major computer manufacturer. The men would then take the chips, sell them to a salvage company, and cash the checks from the salvage company, splitting up the proceeds. The owner of the salvage company assisted the men by writing multiple checks to insure that the amounts were under $10,000. Over the course of approximately 18-24 months, the men sold over $800,000 in stolen memory chips, none of which was reported by any of the men on their tax returns.

As a result of the investigation, four of the men involved pled guilty to charges including conspiracy, money laundering, and tax evasion. They have received sentences of up to 65 months incarceration. They have also been ordered to make restitution to the computer company in an amount over $900,000. The owner of the salvage company was indicted on similar charges and is currently a fugitive. *(Source: IRS/Criminal Investigation)*

State and Local Law Enforcement Use of SAR Data

Following is information obtained through the FinCEN Gateway Program[21] which indicates state and local government's use of SAR data during the period April 1996 through mid-August 2001. Gateway users have the option of identifying (in the system) investigations that were initiated as a result of SAR filings. Because this option is not mandatory, the statistics do not capture the total number of investigative actions initiated by state and local law enforcement or regulatory agencies.

State	Investigations Initiated	State	Investigations Initiated	State	Investigations Initiated	State	Investigations Initiated
AL	2	IL	115	ND	4	PA	170
AR	1	MA	9	NE	2	RI	8
AZ	27	MD	6	NJ	88	SC	3
CA	2	ME	1	NM	3	TX	179
FL	107	MN	5	NV	1	VA	13
GA	2	MO	1	NY	15	WA	1
HI	24	MS	4	OH	6	WI	18
ID	1	NC	1	OR	1	WY	1

[21]The Gateway Program enables federal, state and local law enforcement agencies to have direct, on-line access to records filed under the BSA.

Following are examples of successful investigations conducted by state and local law enforcement agencies that were initiated by SAR filings.

Illegal Casa de Cambio Launders More than $5 Million

In January 1999, the Financial Crimes Division (FCD) of the Texas Office of Attorney General (OAG), initiated an investigation into money laundering allegations based on information received from a Suspicious Activity Report (SAR) filed by a Texas bank. This investigation centered on the operation of an illegal casa de cambio in Dallas and Kaufman Counties, Texas. The subjects of the investigation operated an illegal currency exchange business in violation of the Texas Financial Code, a third degree felony.

Currency exchange and transmission businesses such as casas de cambio may be used by criminals to launder funds in connection with exchanging U.S. dollars for currencies of other countries prior to the funds being transmitted. Money orders in U.S. dollars that are sent to other countries can be difficult to redeem. Many currency exchange and transmission businesses are not licensed to conduct wire transmissions, as is required in many states.

Texas OAG, FCD, researched Bank Secrecy Act (BSA) reports and located a total of 115 Currency Transaction Reports (CTRs), 14 Reports of International Transportation of Currency or Monetary Instruments (CMIRs), two Currency Transaction Reports by Casino (CTRCs) and 11 SARs. The documents helped the investigator by providing specific banking transactions and account information. That information was added to search warrants to establish probable cause and presented to a state grand jury.

The investigation concluded that money orders were received from various senders across the U.S. at the home addresses or post office boxes of the subject. The subject then deposited the money orders into one or more local bank accounts. The banks were then instructed to wire transfer the funds to another out-of-state bank. Information gathered through the use of search warrants determined that from August 1998 through March 1999, banking activity by the casa de cambio included deposits of $5,593,185 and wire transmissions of $5,122,460.

Check Cashing Worker Convicted of Money Laundering

In May 2000, a federal jury convicted an individual from Norwood, Massachusetts, on two counts of money laundering believed to be the proceeds of narcotic sales. At the time of the offense, the individual worked at a Brockton, Massachusetts check cashing business. In May 1998, an undercover Massachusetts State

Trooper, posing as a drug dealer, met with the individual at his place of employment. Using false identification documents and fictitious names, the individual transmitted $18,000 of purported drug proceeds from Brockton to Miami, Florida, where the funds were picked up five days later. A fee of $738 was charged for conducting the transaction. In June 1998, the individual conducted a second money laundering transaction in the amount of $33,000 on behalf of the undercover trooper.

A federal/state task force initiated this investigation. The Massachusetts State Police, Intelligence Unit conducted research on BSA reports relating to the employee of the check cashing business. This research identified 171 CTRs, five CTRCs, two CMIRs and one SAR. The information helped to identify assets, locate bank accounts and was useful in the entire scope of the investigation and prosecution process.

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.

Importance of SAR Reporting to Law Enforcement Investigations

Analysis of SARs plays a critical role in various types of law enforcement investigations. Regardless of the underlying crime, SARs serve as a vital tool for identifying and tracking funds derived from criminal activity. SAR data provides valuable pieces of information that are similar to pieces of a puzzle - each separate piece helps investigators identify complex and sophisticated relationships between people, businesses, locations and assets. Although it is sometimes impossible to obtain 100 percent of the information requested on SAR forms, a concerted effort to obtain specific "puzzle pieces" is very valuable to law enforcement.

Filers should strive to obtain and record as much suspect information as possible. When a suspect exists, always enter suspect related data in the appropriate "Suspect" portion of the form. A recent review of filings indicates that some forms actually contain no identifying names for the suspect but rather have references such as "See Part V" or "See next Page" in the suspect portion of the form. This limits investigative capabilities used to identify suspects and to allow accurate data retrieval/query efforts by law enforcement. Using only a first initial rather than a full first name also poses problems in accurately identifying suspects. Whenever possible, try to obtain complete first names for all suspects. Address information should contain street numbers and apartment numbers if known. Foreign countries should be entered using the attached database standardized country codes. Suspects' occupations also provide high quality leads for law enforcement investigators. When known, vital information should be captured in the suspect area of the SAR form.

Another critical piece of the puzzle is found in identification numbers. Passport numbers should reflect the country of issue in the "Issuing Authority" section

using the standardized country codes. Alien registration numbers contain a letter of the alphabet preceding the actual number – always enter the letter along with the number.

A major element that increases the utility of SARs for law enforcement is the narrative information or "description of activity." If the activity involves wire transfer transactions, include destination city, state and country as well as names of banks and beneficiary persons or businesses. Of particular value are names of foreign financial institutions and the account numbers associated with funds transfers. The use of money orders, traveler's checks, foreign currency or other monetary instruments should also be noted within the activity description. If stocks, bonds, letters of credit, investments, commodities, etc. are involved, this should also be noted as this helps identify methodologies associated with criminal activities.

SAR filers who make reasonable efforts to obtain, record and report the key information outlined above will enhance the ultimate utility of SARs for law enforcement purposes.

Special SAR Form Completion Guidance Related to Computer Intrusion

Part III of the SAR form requires information on the suspicious activity. The following recommendations pertain to Block 35 f. - Computer Intrusion. A SAR should be completed if an incident of computer intrusion has occurred.

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

a. remove, steal, procure or otherwise affect funds of the financial institution or the institution's customers;

b. remove, steal, procure or otherwise affect critical information of the financial institution including customer account information; or

c. damage, disable, disrupt, impair or otherwise affect critical systems of the financial institution.

The perpetrator may be an insider (e.g., an employee of the financial institution) who has misused or overridden his/her authority to access and manipulate customer information. Also, the perpetrator may be an outsider who has somehow

hacked his/her way into the financial institution's critical computer system that contains customer data. In both instances, the use of a computer was involved in committing a crime against a financial institution and its customers.

For purposes of SAR reporting requirements, computer intrusion does not refer to attempted intrusions of websites or other non-critical information systems of the institution. SARs should not be filed for intrusions into systems that provide no access to financial institution information, customer financial information or other critical information.

When an instance of computer intrusion is being reported on a SAR, please ensure that the appropriate violation code of "f" is selected in Part III, block 35 of the SAR form. A detailed explanation of the suspicious activity concerning the computer intrusion should be completed in Part V of the SAR form. This narrative information will provide law enforcement with a valuable weapon against cybercrime as well as information concerning the nature of the fraud that has occurred.

If other types of fraud occur in conjunction with the computer intrusion, please indicate these on the same SAR form in Part III, block 35.

Frequently Asked Questions Regarding Computer Intrusion

(Q) Should a SAR be filed if a financial institution's website is continually "pinged" (attacked) by hacking attempts?

(A) No. If continuous hacking attempts are made against a website, the National Infrastructure Protection Center (NIPC) squad of your local FBI office should be contacted or you may contact the Internet Fraud Complaint Center (IFCC), at (304) 363-4312 or www.ifccfbi.gov.

(Q) Does a financial institution have to file a SAR if an instance of computer intrusion only affects the institution's email system?

(A) No. Since the email system is not linked to financial institution information, customer financial information or other critical information, it will not be necessary to file a SAR. However, the NIPC squad of your local FBI office should be contacted or you may contact the IFCC, at (304) 363-4312 or www.ifccfbi.gov.

(Q) Does a financial institution have to file a SAR if an employee of that institution brings in a diskette containing a computer virus?

(A) No. However, if it can be determined that the employee deliberately intended to use the virus to damage, disable, disrupt, impair or otherwise affect the critical systems of that financial institution, the NIPC squad of your local FBI office should be contacted or you may contact the IFCC, at (304) 363-4312 or www.ifccfbi.gov.

(Q) An employee of a financial institution uses his/her computer access (or that of a co-worker or supervisor) to steal funds from a customer's account. Should a SAR be filed in this instance?

(A) Yes. A SAR would be filed with several violations selected on block 35 of the SAR form, including misuse of position/self dealing, defalcation/embezzlement and computer intrusion.

(Q) A former disgruntled employee of a financial institution uses his/her personal computer to access the institution's critical information system to steal customer account information. Should a SAR be filed to report computer intrusion in this case?

(A) Yes. A SAR should be filed for computer intrusion including any other violations that had affected the customer's financial information (e.g., credit card fraud, identity theft).

(Q) A financial institution's computer server was deliberately infected with a "code red worm" which denied access to online banking customers. Should a computer intrusion SAR be filed in this instance?

(A) Yes. A SAR should be filed and the NIPC squad of your local FBI office should be contacted or you may contact the IFCC, at (304) 363-4312 or www.ifccfbi.gov.

(Q) An employee of a financial institution uses his/her computer to alter a customer's check (or deposit slip) which would affect the deposited funds of the institution's customer. Should a SAR be filed?

(A) Yes. A SAR should be filed with several violations selected on block 35 of the SAR form including misuse of position/self dealing, defalcation/embezzlement, check fraud and computer intrusion.

(Q) A hacker accesses a financial institution's website to post pornographic or other obscene materials on that website. Should a SAR be filed in this instance?

(A) No. The NIPC squad of your local FBI office should be contacted or you may contact the IFCC, at (304) 363-4312 or www.ifccfbi.gov.

(Q) A hacker accesses a financial institution's critical information system to steal customer information and then destroy the data in that institution's information system. Should a SAR be filed?

(A) Yes. A SAR should be filed for computer intrusion including any other violations which had affected the customer's financial information (e.g., credit card fraud, identity theft).

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 financial institution 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 the activity also involved 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 violations being reported.

- In the event the only known or suspected criminal violation detected is identity theft or pretext calling, 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 regarding the preparation and filing of SARs and intends to provide meaningful guidance to filers. This section reflects the collective positions of the government agencies that require organizations to file SARs.

Treasury Establishes Financial Institutions Hotline Relating to Terrorist Activity

On September 26, 2001, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) established a **FINANCIAL INSTITUTIONS HOTLINE, 1-866-556-3974**, for financial institutions to voluntarily report to law enforcement suspicious transactions that may relate to recent terrorist activity against the United States. The purpose of the HOTLINE is to facilitate the immediate transmittal of this information to law enforcement. The HOTLINE will be operational seven days a week, 24 hours a day.

Financial institutions identifying suspicious transactions under 31 CFR Part 103 or under the regulations of their federal financial institution regulators are required to report such transactions by filing a Suspicious Activity Report (SAR) in accordance with applicable agency regulations, even if they provide information over the FINANCIAL INSTITUTIONS HOTLINE. Institutions should file the SAR with the IRS Detroit Computing Center (DCC) as soon as possible. This HOTLINE is intended to provide to law enforcement and other authorized recipients of SAR information the essence of the suspicious activity in an expedited fashion. Using the HOTLINE is voluntary and does not negate an institution's responsibility to file a SAR in accordance with applicable regulations.

Financial institutions identifying such suspicious financial activity on a SAR can assist law enforcement by **(*i*)** capturing the information on the SAR accurately and completely; **(*ii*)** explaining the suspicious transaction as completely as possible in the narrative section; and **(*iii*)** including the following information, if applicable – any correspondent bank name/account information; names/locations of business entities; names of cities, countries and foreign financial institutions linked to the transaction, especially if wire transfer activity is involved; and account numbers and beneficiary names. In addition, institutions preparing SARs are requested to check the "Other" box on Part III, Line 35(s) of the SAR form and to type in "terrorism" immediately following the box.

Information pertaining to the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals List, or questions concerning the financial institution's compliance with OFAC regulations, should be directed to OFAC at its existing hotline at 1-800-540-6322.

Nothing in this announcement precludes a financial institution from directly contacting law enforcement or the institution's federal regulator concerning these issues.

Applicability of Safe Harbor

The BSA safe harbor provision found at 31 U.S.C. § 5318(g)(3) protects financial institutions, and their directors, officers, employees, and agents, from liability for reporting suspicious activity. The safe harbor provision applies even if the report of suspicious activity is made orally or in some form other than through the use of a SAR. In accordance with SAR regulations promulgated by FinCEN and the federal bank supervisory agencies, a bank must make all supporting documentation related to a filed SAR available upon request to appropriate law enforcement agencies, bank supervisory agencies, and FinCEN.

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, ABA Fraud Prevention Oversight Council submits the following:

Recommended Security Procedures for Protecting Customer Information

Background

In 2000, the American Bankers Association issued the "Financial Privacy Toolbox,"[22] an "Identity Theft Prevention and Resolution Kit," and the "Consumer Privacy Training Video" that offered suggested practices for combating the crime of identity theft and pretext calling.[23]

Taking into account those previous recommendations, the advisories issued by the federal banking agencies on reporting identity theft[24] on "Suspicious Activity Reports," as well as the continuing need to prevent bank fraud, the ABA Fraud Prevention Oversight Council offers and restates the following recommended practices for security officers and other appropriate staff to consider when addressing methods on protecting customer information:

Recommended Practices

1. When communicating with customers seeking information on their account, or a third party (such as a merchant or other financial institution) seeking to verify the authenticity of an individual presenting a monetary instrument, or that the presenter has sufficient funds to purchase a product, *a financial institution should consider security measures that:*

---

[22] See, ABA Financial Privacy Toolbox, Tool 5: Training your Employees, available to ABA members on www.aba.com or call 1-800-BANKERS
[23] See, 18 U.S.C. 1028 (federal identity theft statute) and 15 U.S.C. 6821,6823 (federal ban on pretext calling)
[24] See, OCC Advisory Letter 2001-4 (April 30, 2001)

- require the use of a PIN, Password, or some other proper authorization code;
- mandate the use of caller-id or a call-back to the merchant;
- institute some additional mechanism for authentication;[25]
- provide only information that the account exists; or
- prohibit the use of such communication in some instances.

2. When using a third party to investigate a potential fraud, collect on a loan, or to trace lost assets, a financial institution should consider implementing security measures that:

    - require all contacts with those third parties be done via agreement, and require that the third party stipulates that all information received is derived from legal methods and sources, and that the company does not, **in any way,** engage in "pretext calling" or any other unfair and deceptive practice; and

    - require that any third party has security measures designed to protect any consumer information provided to it by the institution, and that the third party stipulates that it will not "reuse or redisclose" any financial information provided by the institution.

3. When training staff to avoid pretext callers, to prevent identity theft against the customer and the institution, and to report possible violations to law enforcement and/or other appropriate regulatory authorities, a financial institution should consider the following measures to ensure compliance with the institution's policies and procedures:

    - Monitor call centers and other customer service representatives to ensure compliance with the institution's security procedures.

    - Consider "footprints" or similar authentication measures on the institution's computers to ensure compliance with the privacy and security policies.

    - Instruct employees not to deviate from customer information security procedures. Once a comprehensive plan has been developed or updated to maintain customer information security— *it*

[25] For example, the ABA Financial Privacy Toolbox suggests routing suspected "pretext calls" to a supervisor or security official. If a call is suspect, you should also consider noting the call for purposes of filing a SAR.

must be adhered to uniformly. Supervisors should demonstrate to frontline personnel that they take the procedures seriously by both following the procedures themselves and enforcing them uniformly within the institution.

- Test your customer information security procedures on a regular basis.

Section 8
Mailbag

In an effort to respond to feedback received concerning various issues of the *SAR Activity Review*, the new "Mailbag" section has been added. Below are some of the questions received from the industry:

(Q) Can FinCEN provide more information on the "Other" Violation category?

(A) Not efficiently. Until better analytical tools are developed, analysis of the SARs where the filer has checked the "Other" violation category would require the retrieval and manual review of each of those 40,000 SARs filed since April 1996. The narrative section for each of those SARs would need to be reviewed manually to identify any notable commonalities or discernable trends.

(Q) Can you provide information on voluntary SAR filings?

(A) Yes. As a result of this question and other inquiries from the filing industries, FinCEN conducted a study to determine the number of SARs filed voluntarily. Those results were provided in the June 2001 *SAR Activity Review* and updated in Section 2 of this issue.

(Q) Can FinCEN provide trend analysis based on geographic areas?

(A) Yes. FinCEN recently created a Geographic Threat Assessment Section (GTAS) that is responsible for identifying trends and patterns based on geographic parameters. Future issues of the *SAR Activity Review* will include items identified by the GTAS.

(Q) Are these publications available on your website?

(A) Yes. FinCEN maintains all issues of the *SAR Activity Review* on our website at **www.fincen**.gov

(Q) Since some sections are useful training tools, how can we download the relevant sections to email to our employees?

(A) It is recommended that you highlight the relevant sections, copy and paste to a word document and then email to your employees.

Appendix 1

Violations by States/Territories by Year

For the Period April 1, 1996 through April 30, 2001

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Alabama																			
1996	77	0	46	38	7	0	8	19	1	1	9	1	23	8	9	2	25	2	27
1997	70	0	67	42	12	0	15	51	0	1	16	1	51	14	19	7	48	1	32
1998	64	1	70	42	12	0	15	23	2	1	16	2	42	10	15	1	48	1	40
1999	81	0	106	58	7	0	10	24	9	1	25	2	53	6	20	2	32	4	60
2000	158	2	129	84	12	2	16	31	3	2	16	2	59	24	25	5	26	2	87
2001	122	1	68	40	4	1	10	17	1	2	16	1	40	13	17	5	13	1	42
Total	572	4	486	304	54	3	74	165	16	8	98	9	268	75	105	22	192	11	288
Alaska																			
1996	39	0	9	5	0	0	0	2	0	0	0	1	2	0	3	0	3	0	4
1997	36	0	6	2	1	0	1	2	0	0	0	0	7	0	1	0	4	0	4
1998	95	0	6	6	0	0	0	2	0	1	1	1	3	2	6	0	3	2	10
1999	119	0	8	6	0	0	0	1	0	2	4	0	4	2	0	0	2	1	12
2000	279	0	14	11	2	0	3	2	0	4	4	2	6	3	1	1	4	3	24
2001	95	0	5	0	0	0	1	2	0	0	4	0	1	1	0	0	0	2	7
Total	663	0	48	30	3	0	5	11	0	7	13	4	23	8	11	1	16	8	61

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
American Samoa																			
1996	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0
1997	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1998	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	0
1999	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1
2000	1	0	0	0	0	0	0	0	0	0	0	0	2	0	1	0	1	0	3
2001	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Total	1	0	0	0	0	0	0	1	0	0	0	0	13	0	1	0	1	0	4
Arizona																			
1996	361	0	187	71	3	0	87	38	12	4	212	7	82	73	13	9	8	2	53
1997	592	0	257	51	3	0	52	138	24	1	324	23	146	54	27	10	4	4	76
1998	949	0	298	33	2	0	19	178	34	6	452	22	101	23	31	10	13	3	132
1999	1,515	0	255	44	8	0	30	192	1	1	162	20	80	30	35	30	7	6	134
2000	1,602	0	393	94	6	0	22	200	24	6	736	54	117	60	33	49	15	12	469
2001	986	0	254	38	7	0	9	106	6	3	37	15	90	28	22	23	10	5	191
Total	6,005	0	1,644	331	29	0	219	852	101	21	1,923	141	616	268	161	131	57	32	1,055

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Arkansas																			
1996	44	0	22	19	6	0	3	4	0	1	4	0	23	6	21	0	26	6	23
1997	77	2	35	31	22	0	9	5	0	1	2	2	38	27	16	6	21	2	26
1998	78	1	38	34	11	0	9	6	0	2	16	0	39	12	9	2	22	0	44
1999	91	0	118	56	18	0	18	16	0	3	15	1	32	12	18	7	18	6	110
2000	116	5	92	43	27	2	12	43	0	1	8	2	26	14	24	4	39	8	83
2001	61	2	29	27	16	0	8	9	0	0	8	0	21	13	12	9	25	7	35
Total	467	10	334	210	100	2	59	83	0	8	53	5	179	84	100	28	151	29	321
California																			
1996	5,241	12	2,438	278	58	0	281	767	17	13	78	25	767	512	112	682	61	35	536
1997	8,969	11	2,839	400	107	0	475	1,150	23	23	185	81	1,202	535	168	935	161	52	816
1998	13,284	12	3,019	460	96	0	394	1,214	20	26	267	93	1,252	425	180	712	215	59	1,151
1999	16,155	10	2,979	332	165	0	545	865	30	37	396	174	984	610	153	572	120	100	963
2000	30,118	13	3,926	447	136	10	774	1,460	135	52	559	221	1,029	800	199	566	138	105	1,027
2001	16,547	6	1,877	275	43	10	794	668	80	11	207	87	492	202	78	365	58	83	802
Total	90,314	64	17,078	2,192	605	20	3,263	6,124	305	162	1,692	681	5,726	3,084	890	3,832	753	434	5,295

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Colorado																			
1996	275	0	156	34	2	0	15	58	5	0	20	5	45	22	11	5	24	1	52
1997	403	2	257	58	6	0	15	48	3	3	7	7	45	16	16	4	28	3	158
1998	560	10	276	56	4	0	11	80	1	2	22	6	76	18	26	19	39	37	102
1999	797	0	206	91	3	0	13	77	7	2	42	13	61	16	16	16	24	2	94
2000	922	2	273	119	13	2	18	154	3	3	40	10	80	35	31	29	38	4	101
2001	514	0	165	62	9	4	11	85	1	1	20	12	61	21	21	27	19	5	77
Total	3,471	14	1,333	420	37	6	83	502	20	11	151	53	368	128	121	100	172	52	584
Connecticut																			
1996	149	0	60	30	5	0	9	12	0	1	2	0	26	6	11	4	15	1	56
1997	360	0	109	56	5	0	18	25	0	0	21	0	59	13	9	5	14	2	74
1998	472	0	108	53	4	0	29	38	0	2	20	3	45	34	14	11	23	5	69
1999	567	1	71	40	7	0	11	48	0	0	12	1	35	23	5	17	13	8	173
2000	836	0	157	34	7	0	8	63	4	3	21	7	32	12	9	16	31	2	70
2001	357	1	57	14	2	0	6	23	3	0	5	2	15	6	4	8	13	3	20
Total	2,741	2	562	227	30	0	81	209	7	6	81	13	212	94	52	61	109	21	462

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Delaware																			
1996	12	0	28	12	0	0	1	30	4	1	153	1	5	5	8	2	0	0	57
1997	42	0	54	51	0	0	1	108	7	8	410	1	11	6	9	1	1	5	67
1998	36	0	54	6	3	0	6	174	1	2	372	4	12	9	10	0	3	5	69
1999	156	1	82	18	4	0	12	231	8	3	482	5	23	8	8	0	6	5	137
2000	121	0	358	1,071	6	1	6	473	34	21	739	106	22	12	8	1	3	109	145
2001	55	0	165	449	0	1	2	127	28	6	372	3	9	5	5	0	2	13	94
Total	422	1	741	1,607	13	2	28	1,143	82	41	2,528	120	82	45	48	4	15	137	569
District of Columbia																			
1996	53	0	35	12	0	0	6	10	0	2	0	2	14	3	2	1	5	1	8
1997	66	1	35	12	1	0	2	12	0	1	5	0	13	6	1	0	10	3	19
1998	80	0	32	6	3	0	5	16	0	3	2	2	34	6	1	0	7	6	17
1999	143	0	21	3	1	0	1	19	0	0	3	1	14	4	3	3	1	1	16
2000	230	0	63	9	4	0	11	46	3	1	1	7	36	11	10	9	5	4	47
2001	143	0	35	4	0	0	3	25	0	1	1	0	7	8	4	3	2	5	31
Total	715	1	221	46	9	0	28	128	3	8	12	12	118	38	21	16	30	20	138

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Federated States of Micronesia																			
1996	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
1997	0	0	1	1	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2
1998	1	0	1	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	1
1999	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
2000	0	0	1	0	0	0	0	1	0	1	0	0	0	0	2	0	0	0	1
2001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Total	1	0	3	1	0	0	0	1	0	1	0	0	4	0	4	0	0	0	4
Florida																			
1996	2,302	8	672	158	19	0	51	34	0	8	11	14	105	69	39	44	67	17	200
1997	4,108	8	864	219	20	0	108	117	3	13	45	11	186	108	49	54	85	19	306
1998	4,748	4	530	113	13	0	62	168	7	17	139	11	162	53	59	76	63	26	336
1999	4,929	8	649	158	30	0	86	431	7	14	239	14	195	93	76	266	83	19	467
2000	5,527	10	911	240	44	2	226	476	89	18	146	69	289	150	97	301	129	42	676
2001	3,142	4	425	96	32	5	34	164	56	7	90	20	105	45	27	198	28	37	275
Total	24,756	42	4,051	984	158	7	567	1,390	162	77	670	139	1,042	518	347	939	455	160	2,260

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Georgia																			
1996	207	1	68	36	7	0	20	15	0	2	74	2	60	25	17	13	28	5	66
1997	426	3	210	84	16	0	24	48	2	7	174	6	92	46	39	34	73	8	104
1998	627	2	220	63	30	0	49	87	1	9	82	11	121	53	52	22	82	8	139
1999	870	0	226	61	16	0	49	163	4	11	119	7	108	54	45	67	84	6	122
2000	1,175	4	530	86	22	0	58	350	16	3	69	37	124	54	46	90	87	29	287
2001	554	4	287	51	7	3	43	166	11	3	40	15	63	15	23	43	29	13	119
Total	3,859	14	1,541	381	98	3	243	829	34	35	558	78	568	247	222	269	383	69	837
Guam																			
1996	5	0	5	0	1	0	0	0	0	0	0	0	1	2	1	0	0	1	6
1997	18	0	10	1	0	0	3	0	0	0	0	0	6	0	2	0	2	1	14
1998	29	0	6	2	0	0	0	0	0	0	0	0	2	1	2	0	1	1	8
1999	47	4	5	4	0	0	0	0	0	0	0	1	3	4	7	0	1	0	17
2000	35	1	9	5	1	0	0	0	0	1	0	0	6	3	5	0	0	0	10
2001	15	0	1	1	1	0	0	1	0	1	0	0	2	0	3	0	0	1	2
Total	149	5	36	13	3	0	3	1	0	2	0	1	20	10	20	0	4	4	57

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Hawaii																			
1996	224	0	44	6	2	0	0	10	0	1	2	1	24	6	4	1	5	1	62
1997	336	0	38	11	1	0	8	5	1	0	16	1	29	5	3	0	5	2	78
1998	357	1	37	4	0	0	0	19	3	0	16	3	16	4	3	0	2	1	85
1999	350	0	31	4	1	0	3	13	4	0	7	0	16	0	7	0	10	1	58
2000	474	3	30	10	2	0	4	12	2	1	11	1	16	3	7	1	5	1	44
2001	333	0	21	12	0	0	1	16	0	0	4	2	6	0	0	0	0	0	12
Total	2,074	4	201	47	6	0	16	75	10	2	56	8	107	18	24	2	27	6	339
Idaho																			
1996	11	0	17	7	1	0	1	4	0	0	1	0	7	2	1	3	1	0	3
1997	37	0	31	15	2	0	3	1	0	0	3	2	20	7	7	1	4	1	12
1998	42	0	19	12	2	0	1	7	0	0	4	0	14	1	2	3	1	0	10
1999	60	0	34	19	2	0	4	17	0	0	3	0	16	3	11	2	1	1	20
2000	223	0	32	23	1	0	4	6	0	1	2	1	17	8	3	5	7	1	9
2001	70	1	25	13	0	1	6	4	0	0	0	3	20	5	0	2	2	0	11
Total	443	1	158	89	8	1	19	39	0	1	13	6	94	26	24	16	16	3	65

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Illinois																			
1996	279	6	290	102	32	0	21	41	0	8	14	4	96	28	39	35	62	6	115
1997	563	5	655	208	36	0	41	96	7	9	49	21	203	64	60	40	91	17	200
1998	663	5	632	174	39	0	41	105	1	3	51	14	182	75	68	56	114	16	208
1999	1,013	9	932	172	53	0	84	270	2	17	123	19	243	44	98	78	148	30	225
2000	1,475	3	755	184	55	6	133	377	40	78	85	31	316	88	81	133	106	34	331
2001	766	1	454	119	22	8	27	165	11	65	50	12	179	43	47	101	36	38	183
Total	4,759	29	3,718	959	237	14	347	1,054	61	180	372	101	1,219	342	393	443	557	141	1,262
Indiana																			
1996	148	2	58	35	8	0	12	4	1	5	5	1	56	19	10	0	26	2	62
1997	265	0	75	44	10	0	20	12	2	0	23	6	94	17	16	2	40	5	79
1998	374	0	95	54	12	0	35	20	1	0	6	5	94	17	32	7	32	3	125
1999	458	2	179	60	12	0	30	89	0	4	16	5	97	23	33	5	71	2	128
2000	498	2	170	57	19	0	25	94	3	0	19	8	99	33	43	28	71	7	117
2001	254	0	98	30	7	0	12	36	1	1	14	2	50	21	23	16	36	9	46
Total	1,997	6	675	280	68	0	134	255	8	10	83	27	490	130	157	58	276	28	557

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Iowa																			
1996	31	0	20	60	3	0	1	3	0	0	2	1	14	10	8	1	9	3	29
1997	77	0	21	53	10	0	8	4	0	1	5	10	20	16	7	1	8	3	46
1998	86	1	23	47	8	0	7	0	1	1	3	2	18	12	12	0	7	2	40
1999	145	0	37	42	15	0	6	14	2	1	6	6	26	15	9	3	9	4	40
2000	182	0	34	34	11	1	1	11	1	0	10	4	12	12	6	5	10	4	48
2001	91	1	38	16	6	1	3	20	0	0	10	0	20	8	8	3	6	4	46
Total	612	2	173	252	53	2	26	52	4	3	36	23	110	73	50	13	49	20	249
Kansas																			
1996	50	0	25	10	10	0	7	2	0	1	1	0	17	10	2	1	10	0	53
1997	59	0	40	17	13	0	10	7	1	1	16	0	24	14	8	4	14	1	36
1998	109	0	49	22	14	0	7	4	0	1	5	0	38	13	9	4	26	6	31
1999	143	0	96	47	11	0	9	20	0	2	14	2	47	12	17	7	32	2	49
2000	130	1	60	26	30	3	7	14	1	3	7	1	29	20	15	13	28	9	44
2001	78	0	25	20	12	0	6	10	0	3	12	3	19	15	6	17	26	2	18
Total	569	1	295	142	90	3	46	57	2	11	55	6	174	84	57	46	136	20	231

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Kentucky																			
1996	76	1	43	11	7	0	6	6	0	2	4	5	19	6	8	2	27	3	28
1997	90	0	67	23	13	0	18	3	0	1	6	3	53	6	24	1	26	1	48
1998	127	0	64	53	13	0	9	11	0	1	7	3	55	15	18	1	14	8	50
1999	199	0	64	40	20	0	19	30	0	0	16	4	49	30	24	5	27	2	62
2000	278	2	85	40	12	0	24	24	0	1	4	5	53	22	30	2	20	2	68
2001	146	0	48	56	8	0	5	14	0	1	13	3	32	15	12	1	10	8	34
Total	916	3	371	223	73	0	81	88	0	6	50	23	261	94	116	12	124	24	290
Louisiana																			
1996	154	1	64	59	8	0	6	13	0	0	8	4	41	11	11	10	26	3	56
1997	144	4	98	70	22	0	21	11	0	3	27	4	73	24	29	0	33	7	45
1998	188	0	96	77	9	0	17	75	1	2	21	5	75	23	36	5	27	3	82
1999	282	0	130	88	21	0	12	54	0	3	25	3	66	41	43	3	27	8	81
2000	1,122	0	142	70	18	1	39	57	1	0	24	1	83	41	55	8	48	5	85
2001	563	1	71	40	14	0	20	28	1	2	16	0	42	15	17	2	27	4	35
Total	2,453	6	601	404	92	1	115	238	3	10	121	17	380	155	191	28	188	30	384

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Maine																			
1996	28	0	11	31	3	0	8	5	0	0	3	1	3	5	1	0	4	2	15
1997	52	0	33	32	5	0	7	2	0	1	4	4	2	9	5	2	4	3	21
1998	58	1	51	20	1	0	3	8	1	0	3	1	8	4	7	2	11	3	9
1999	63	0	28	28	4	0	3	8	1	1	7	4	15	2	6	1	12	9	17
2000	92	0	29	23	4	0	2	12	0	0	5	0	7	5	5	3	11	0	9
2001	41	1	27	25	2	0	2	7	0	1	4	1	5	1	3	0	8	2	12
Total	334	2	179	159	19	0	25	42	2	3	26	11	40	26	27	8	50	19	83
Marshall Islands																			
1996	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1997	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1998	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1999	0	0	0	0	0	0	0	0	0	0	0	0	2	0	1	0	0	0	0
2000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2001	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Total	0	0	0	0	0	0	0	0	0	0	0	0	3	0	1	0	0	0	0

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Maryland																			
1996	235	0	121	37	9	0	10	11	0	2	10	1	55	19	10	15	23	6	40
1997	367	1	155	43	14	0	8	22	0	2	20	4	84	41	15	46	24	4	69
1998	583	0	132	47	8	0	14	42	0	7	20	10	103	36	19	47	27	4	85
1999	792	0	131	34	3	0	12	73	0	1	34	4	84	18	13	156	46	3	83
2000	842	0	265	59	5	0	16	155	4	2	22	17	130	49	19	267	63	7	144
2001	405	0	123	33	2	0	8	58	2	1	21	10	49	14	12	106	23	9	79
Total	3,224	1	927	253	41	0	68	361	6	15	127	46	505	177	88	637	206	33	500
Massachusetts																			
1996	384	1	34	22	5	0	11	26	0	0	3	4	36	15	7	6	8	3	85
1997	732	0	151	57	8	0	14	26	0	3	10	2	84	26	33	16	16	8	72
1998	936	0	291	61	14	0	11	50	1	2	14	2	70	28	20	11	20	15	116
1999	1,639	1	251	56	17	0	14	80	7	6	21	13	73	24	26	8	24	14	86
2000	1,763	0	317	38	11	5	10	129	3	2	17	21	59	57	15	22	35	21	156
2001	695	0	245	16	6	1	18	60	2	2	6	7	45	31	15	20	16	7	69
Total	6,149	2	1,289	250	61	6	78	371	13	15	71	49	367	181	116	83	119	68	584

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Michigan																			
1996	206	3	195	119	10	0	33	41	2	8	8	10	108	25	28	5	55	3	130
1997	279	3	281	226	23	0	30	101	1	3	27	17	225	48	60	7	83	8	141
1998	258	5	259	202	21	0	25	146	1	4	77	4	225	60	72	12	94	4	143
1999	621	0	404	131	13	0	61	214	1	6	174	24	222	92	73	44	89	8	171
2000	993	2	539	149	20	1	73	284	13	4	40	43	239	154	100	386	124	16	206
2001	729	3	363	82	7	2	30	154	4	2	47	35	98	59	26	191	37	5	69
Total	3,086	16	2,041	909	94	3	252	940	22	27	373	133	1,117	438	359	645	482	44	860
Minnesota																			
1996	562	1	130	29	2	0	5	9	0	0	3	6	32	15	22	2	22	2	44
1997	1,404	0	286	59	21	0	4	23	1	3	5	17	41	28	30	8	37	6	185
1998	1,180	2	554	80	16	0	13	57	2	4	13	22	61	19	28	0	26	3	102
1999	851	1	707	117	15	0	21	112	1	4	16	60	92	26	37	10	26	2	56
2000	1,224	8	515	98	18	0	29	123	2	6	24	53	73	28	58	10	49	8	65
2001	461	3	261	56	6	2	7	50	1	0	21	38	44	13	30	4	24	6	81
Total	5,682	15	2,453	439	78	2	79	374	7	17	82	196	343	129	205	34	184	27	533

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Mississippi																			
1996	23	0	17	31	3	0	5	4	0	0	0	1	25	5	18	1	6	2	10
1997	47	1	31	42	7	0	6	4	0	0	9	0	26	13	19	2	8	0	17
1998	36	0	29	49	5	0	4	3	0	0	7	3	16	5	11	0	6	1	23
1999	62	0	24	30	13	0	6	9	0	1	5	0	53	34	38	3	12	1	23
2000	263	1	38	39	15	0	11	9	2	2	9	2	41	33	31	7	8	6	55
2001	141	0	21	20	6	0	7	9	0	1	6	1	25	16	18	3	6	0	21
Total	572	2	160	211	49	0	39	38	2	4	36	7	186	106	135	16	46	10	149
Missouri																			
1996	130	0	107	34	13	0	8	11	0	4	18	2	44	28	20	7	35	2	43
1997	155	0	247	53	30	0	17	29	6	2	51	16	79	31	28	7	58	9	79
1998	194	0	299	37	33	0	15	47	6	3	29	13	114	23	36	25	62	4	122
1999	211	0	253	71	25	0	14	101	6	1	35	14	115	18	43	13	58	8	112
2000	328	3	216	61	44	1	44	84	3	5	34	13	127	87	53	86	63	11	237
2001	192	1	116	42	19	3	50	72	2	1	14	8	61	33	28	60	43	9	133
Total	1,210	4	1,238	298	164	4	148	344	23	16	181	66	540	220	208	198	319	43	726

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Montana																			
1996	22	0	2	8	1	0	1	1	0	0	0	0	4	2	7	2	3	0	10
1997	26	0	6	7	4	0	5	3	0	0	1	3	9	3	4	0	5	2	9
1998	38	0	6	4	1	0	3	5	0	0	0	2	8	4	3	1	3	0	11
1999	49	0	16	5	0	0	4	8	0	0	1	0	10	2	1	0	5	0	16
2000	93	0	20	14	0	0	2	21	0	0	0	0	9	4	1	1	4	3	6
2001	42	0	11	9	2	0	1	5	0	1	2	1	6	5	4	0	1	0	16
Total	270	0	61	47	8	0	16	43	0	1	4	6	46	20	20	4	21	5	68
Nebraska																			
1996	53	2	28	6	1	0	3	4	0	2	0	0	12	5	4	0	3	0	19
1997	46	0	33	14	5	0	5	2	1	0	3	1	27	16	11	1	10	3	24
1998	108	0	46	19	5	0	7	7	2	0	7	2	14	16	4	1	6	3	32
1999	122	1	63	19	10	0	8	8	0	0	19	0	21	12	4	3	13	2	22
2000	241	1	105	45	7	1	12	12	0	0	3	5	28	15	20	4	11	2	32
2001	108	0	52	48	7	1	6	13	2	1	3	1	14	13	5	2	2	1	18
Total	678	4	327	151	35	2	41	46	5	3	35	9	116	77	48	11	45	11	147

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Nevada																			
1996	322	0	93	51	2	0	18	7	0	1	11	1	38	31	8	27	4	2	18
1997	615	0	158	56	4	0	416	43	1	3	9	4	59	20	13	12	5	6	56
1998	711	2	204	39	6	0	709	75	1	3	26	4	66	25	12	1	5	3	75
1999	860	0	266	47	16	0	445	134	4	3	43	10	64	25	18	14	13	4	96
2000	1,173	0	335	182	9	0	534	177	22	6	230	28	90	23	16	44	26	6	111
2001	607	0	161	195	1	0	8	72	3	2	105	11	27	10	5	6	9	2	95
Total	4,288	2	1,217	570	38	0	2,130	508	31	18	424	58	344	134	72	104	62	23	451
New Hampshire																			
1996	43	0	17	5	2	0	0	1	0	0	3	0	4	1	0	0	2	1	3
1997	59	0	27	12	2	0	0	2	0	2	0	3	19	1	7	0	3	0	10
1998	89	0	31	13	3	0	2	9	0	1	4	1	6	3	1	3	19	0	16
1999	97	0	132	17	0	0	3	1	20	0	20	1	15	1	4	2	25	0	19
2000	125	0	44	12	1	0	2	8	2	0	4	1	5	4	3	1	12	2	9
2001	64	0	35	4	0	0	1	6	0	0	4	2	3	0	5	2	4	4	14
Total	477	0	286	63	8	0	8	27	22	3	35	8	52	10	20	8	65	7	71

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
New Jersey																			
1996	343	1	174	20	4	0	9	36	1	1	3	5	71	24	18	13	41	7	149
1997	629	1	271	48	6	0	11	87	2	2	40	3	118	44	30	34	41	10	236
1998	1,101	2	321	66	20	0	19	125	0	9	29	3	137	27	17	18	71	8	297
1999	1,811	2	340	70	16	0	28	143	3	4	66	8	138	22	20	39	56	13	143
2000	2,219	0	604	79	12	2	29	174	27	6	66	20	217	47	36	80	71	25	308
2001	1,018	0	327	38	5	1	8	58	28	8	35	8	81	12	15	34	39	16	98
Total	7,121	6	2,037	321	63	3	104	623	61	30	239	47	762	176	136	218	319	79	1,231
New Mexico																			
1996	75	0	35	9	1	0	4	10	0	0	2	2	29	7	11	3	14	0	25
1997	67	0	64	12	2	0	0	9	0	1	4	1	23	3	4	0	13	2	32
1998	127	1	40	27	1	0	0	8	0	0	2	2	28	3	11	0	19	2	13
1999	137	0	43	20	7	0	2	13	0	2	2	1	16	6	7	1	10	1	32
2000	147	0	48	9	1	1	12	14	1	0	2	1	17	8	10	2	9	1	35
2001	91	0	22	8	1	0	5	7	0	0	7	1	13	5	5	2	8	0	19
Total	644	1	252	85	13	1	23	61	1	3	19	8	126	32	48	8	73	6	156

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
New York																			
1996	2,448	17	578	201	39	0	33	199	5	24	23	17	174	53	41	22	61	23	601
1997	4,905	18	1,012	286	86	0	37	434	5	35	89	22	279	124	95	37	100	59	813
1998	6,998	10	1,195	328	75	0	30	640	2	48	88	16	247	185	73	20	106	56	1,169
1999	9,93	15	1,521	295	125	0	66	523	60	49	261	25	240	112	92	54	93	79	688
2000	12,250	10	1,652	259	70	5	107	733	60	47	203	38	241	108	68	139	85	107	869
2001	5,887	10	1,221	103	28	12	186	490	28	38	105	21	130	46	23	83	40	78	624
Total	42,422	80	7,179	1,472	423	17	459	3,019	160	241	769	139	1,311	628	392	355	485	402	4,764
North Carolina																			
1996	317	1	113	69	3	0	8	22	0	3	78	0	57	16	23	3	32	5	75
1997	597	0	221	139	15	0	42	92	7	2	35	7	81	40	48	25	71	12	118
1998	811	1	222	138	14	0	42	126	2	6	30	3	110	42	47	26	95	11	172
1999	848	0	310	174	21	0	60	184	1	8	62	8	113	51	88	21	58	18	170
2000	1,176	2	357	189	24	0	120	195	6	5	50	7	129	63	78	143	71	23	237
2001	423	0	156	71	13	2	27	57	1	3	26	8	48	19	25	46	19	7	93
Total	4,172	4	1,379	780	90	2	299	676	17	27	281	33	538	231	309	264	346	76	865

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
North Dakota																			
1996	5	0	6	2	3	0	4	0	0	0	1	0	1	3	2	0	1	0	3
1997	142	1	21	8	7	0	3	0	0	0	3	2	4	3	4	0	1	0	8
1998	143	1	14	13	6	0	3	1	0	0	2	0	5	9	3	0	1	0	5
1999	38	0	16	10	8	0	6	3	0	0	2	1	4	4	2	2	3	1	10
2000	66	0	11	19	11	0	4	9	0	0	2	1	3	6	9	3	3	1	12
2001	15	0	5	5	1	2	0	4	0	0	1	0	2	1	4	1	0	0	5
Total	409	2	73	57	36	2	20	17	0	0	11	4	19	26	24	6	9	2	43
Northern Mariana Islands																			
1996	14	0	2	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	4
1997	1	0	1	2	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1
1998	3	0	4	2	0	0	0	0	0	0	0	0	1	0	1	0	0	0	4
1999	18	0	4	4	0	0	0	0	0	0	1	1	1	1	1	0	2	1	2
2000	51	0	0	0	0	0	0	0	0	0	0	1	2	0	0	0	0	2	2
2001	21	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	0	0	0
Total	108	0	11	9	0	0	0	0	0	0	1	2	7	3	4	0	2	3	13

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Ohio																			
1996	179	1	122	79	10	0	21	20	0	5	13	6	102	16	28	5	31	3	85
1997	352	1	250	165	11	0	49	37	5	6	82	14	179	21	49	5	74	5	145
1998	731	2	269	193	16	0	45	110	3	3	49	18	206	33	63	4	86	7	179
1999	565	7	333	244	20	0	49	174	2	7	98	16	202	56	91	39	89	13	165
2000	862	1	458	408	20	3	61	253	97	16	200	44	232	63	94	86	112	20	177
2001	478	3	176	168	9	3	48	84	106	3	155	4	104	56	62	249	46	18	129
Total	3,167	15	1,608	1,257	86	6	273	678	213	40	597	102	1,025	245	387	388	438	66	880
Oklahoma																			
1996	124	0	23	73	12	0	2	6	1	4	0	0	22	8	9	0	9	1	31
1997	162	3	37	47	22	0	6	9	1	4	6	3	34	15	12	0	14	1	35
1998	155	0	52	43	25	0	4	9	0	1	10	0	36	10	8	1	8	16	44
1999	205	0	113	44	22	0	25	22	0	3	11	6	60	32	16	6	11	5	67
2000	201	1	111	48	16	1	8	32	1	3	25	9	67	20	25	5	23	2	87
2001	107	0	31	19	6	0	6	5	0	0	15	1	28	7	6	4	9	4	33
Total	954	4	367	274	103	1	51	83	3	15	67	19	247	92	76	16	74	29	297

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Oregon																			
1996	178	1	133	22	2	0	17	26	1	1	1	4	49	12	9	3	9	1	28
1997	330	0	253	86	4	0	13	57	0	2	14	16	94	25	19	8	16	1	103
1998	432	0	269	76	4	0	3	151	1	1	12	16	58	8	6	6	4	9	68
1999	593	1	369	97	9	0	18	432	2	2	47	13	69	40	11	9	13	3	101
2000	1,470	2	383	87	12	1	13	141	5	2	14	15	69	34	14	17	10	8	56
2001	502	1	178	50	2	0	26	56	3	0	12	6	27	24	6	11	15	5	55
Total	3,505	5	1,585	418	33	1	90	863	12	8	100	70	366	143	65	54	67	27	411
Overseas																			
1996	9	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	1
1997	32	0	2	0	0	0	0	1	0	0	3	0	1	0	0	0	0	1	1
1998	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	2
1999	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2000	3	0	2	0	1	0	0	1	0	0	0	2	1	0	0	0	1	3	9
2001	1	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	2	1
Total	48	0	6	0	2	0	0	4	1	0	3	2	3	0	1	0	1	6	14

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Pennsylvania																			
1996	459	1	164	67	4	0	25	62	0	3	11	10	54	24	16	10	34	10	98
1997	861	5	409	108	20	0	29	199	4	3	68	21	134	55	55	18	80	24	197
1998	822	1	298	95	24	0	28	169	1	4	42	13	106	35	33	34	42	16	215
1999	1,513	0	343	99	17	0	41	154	12	8	53	19	122	34	38	46	47	14	200
2000	1,461	2	483	127	20	1	69	195	5	5	45	33	203	56	44	72	73	8	217
2001	809	1	224	73	19	5	22	61	4	6	35	9	71	32	37	21	26	10	108
Total	5,925	10	1,921	569	104	6	214	840	26	29	254	105	690	236	223	201	302	82	1,035
Puerto Rico																			
1996	95	1	4	1	3	0	8	2	2	2	2	0	10	6	13	2	5	1	9
1997	472	0	21	8	6	0	4	2	0	3	15	3	11	7	14	0	7	4	11
1998	347	2	20	8	0	0	13	6	0	0	12	6	15	5	14	0	4	3	44
1999	230	0	23	7	0	0	2	4	0	1	12	3	15	14	3	1	2	2	22
2000	595	7	156	29	6	1	23	11	3	0	72	37	25	29	17	5	7	4	51
2001	347	2	29	4	1	1	2	3	1	0	25	11	8	5	3	0	1	5	23
Total	2,086	12	253	57	16	2	52	28	6	6	138	60	84	66	64	8	26	19	160

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Rhode Island																			
1996	70	0	23	6	2	0	2	3	0	0	3	1	4	5	1	0	7	0	10
1997	124	0	38	12	2	0	10	17	0	2	6	0	2	8	0	1	6	0	20
1998	134	0	33	15	2	0	15	14	0	0	6	0	6	7	3	4	2	0	15
1999	248	0	37	9	1	0	8	13	0	0	10	1	4	6	4	1	1	0	10
2000	277	0	76	16	0	1	2	16	1	2	7	8	25	4	8	5	7	0	11
2001	82	0	51	7	1	0	1	9	0	0	6	0	6	1	2	0	0	0	6
Total	935	0	258	65	8	1	38	72	1	4	38	10	47	31	18	11	23	0	72
South Carolina																			
1996	139	0	28	18	2	0	8	7	0	1	6	0	25	9	4	0	13	0	22
1997	220	1	71	31	9	0	14	21	0	2	12	3	56	14	21	12	37	3	48
1998	252	0	57	31	4	0	11	32	0	1	14	3	28	8	17	102	18	0	50
1999	281	3	60	30	1	0	10	43	1	1	17	2	49	13	26	31	35	4	56
2000	289	1	117	52	6	0	13	40	2	1	21	1	28	13	11	35	15	5	56
2001	130	0	60	30	2	0	8	23	1	2	18	5	30	9	14	13	24	1	51
Total	1,311	5	393	192	24	0	64	166	4	8	88	14	216	66	93	193	142	13	283

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
South Dakota																			
1996	8	0	5	3	3	0	2	1	3	3	258	0	5	3	2	0	6	1	4
1997	56	0	17	11	2	0	1	0	2	0	308	3	10	4	3	0	3	1	10
1998	32	0	16	76	6	0	2	7	1	1	280	2	9	8	11	0	3	1	19
1999	30	1	22	12	4	0	2	7	0	1	23	0	9	7	14	0	6		7
2000	52	0	19	19	5	0	5	4	1	1	5	0	12	5	2	0	7	2	9
2001	39	1	15	15	2	0	2	4	0	2	9	0	6	5	2	0	6	2	10
Total	217	2	94	136	22	0	14	23	7	8	883	5	51	32	34	0	31	7	59
Tennessee																			
1996	148	1	61	98	10	0	15	3	0	2	7	1	53	14	15	0	27	2	45
1997	254	1	83	142	28	0	26	18	2	2	16	2	85	21	36	4	42	3	60
1998	298	2	109	72	16	0	31	33	0	3	9	4	103	60	43	7	23	4	89
1999	312	1	109	61	20	0	36	39	1	1	26	4	107	58	60	12	47	5	84
2000	697	3	160	82	7	4	35	56	3	5	29	6	99	55	45	27	36	5	150
2001	394	4	75	62	11	0	29	33	0	1	25	2	63	37	46	50	8	1	59
Total	2,103	12	597	517	92	4	172	182	6	14	112	19	510	245	245	100	183	20	487

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Texas																			
1996	1,863	2	426	115	31	0	46	127	0	9	36	13	168	87	53	21	119	25	345
1997	2,411	2	550	176	46	0	50	116	3	30	129	22	284	82	75	32	115	28	326
1998	3,557	3	605	192	45	0	88	228	5	11	121	8	297	93	76	26	111	24	410
1999	4,476	5	639	212	57	0	263	267	2	19	164	19	307	111	106	66	115	38	380
2000	5,413	10	853	262	61	3	322	392	43	19	128	39	330	126	110	206	177	40	450
2001	3,548	3	547	177	37	4	127	266	12	9	83	27	144	80	59	88	45	23	369
Total	21,268	25	3,620	1,134	277	7	896	1,396	65	97	661	128	1,530	579	479	439	682	178	2,280
U.S. Virgin Islands																			
1996	0	0	1	0	0	0	0	0	0	0	0	0	1	1	2	0	0	0	0
1997	4	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1
1998	8	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	1	0
1999	5	0	1	4	0	0	0	0	0	0	2	0	2	0	0	0	1	0	0
2000	22	0	0	0	0	0	1	0	0	1	1	0	3	1	3	0	0	0	0
2001	17	0	1	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1
Total	56	0	4	5	0	0	2	2	0	1	4	0	9	2	5	0	1	1	2

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Utah																			
1996	27	0	29	16	1	0	12	3	0	1	121	0	15	7	8	0	1	0	22
1997	148	0	71	28	4	0	19	9	0	2	460	4	44	13	16	2	2	3	232
1998	274	1	61	24	2	0	11	11	0	0	438	4	52	16	19	48	9	8	360
1999	411	1	84	23	3	0	6	21	0	8	599	1	32	25	18	12	1	2	558
2000	607	0	139	44	6	0	11	45	7	4	1,133	58	32	80	16	25	10	4	1,118
2001	266	0	274	18	1	0	16	41	16	9	619	106	18	23	11	9	3	4	613
Total	1,733	2	658	153	17	0	75	130	23	24	3,370	173	193	164	88	96	26	21	2,903
Vermont																			
1996	14	0	11	9	0	0	1	0	0	0	0	0	4	4	2	0	1	1	4
1997	27	0	19	3	6	0	3	2	0	0	3	3	10	5	5	1	1	1	3
1998	15	0	11	3	3	0	2	0	1	0	7	0	4	2	5	0	6	0	6
1999	17	0	3	7	0	0	3	1	1	0	6	1	5	3	2	1	5	1	3
2000	29	0	6	6	0	0	1	5	0	0	1	1	2	2	2	0	0	1	7
2001	13	0	9	4	1	2	1	0	0	0	2	0	1	1	1	0	1	0	8
Total	115	0	59	32	10	2	11	8	2	0	19	5	26	17	17	2	14	4	31

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Virginia																			
1996	109	1	76	38	10	0	16	13	1	0	35	2	45	14	19	10	28	5	53
1997	279	0	151	70	11	0	57	24	2	3	79	2	115	38	39	25	31	8	78
1998	484	6	157	99	11	0	26	76	2	5	54	5	136	22	42	51	51	14	102
1999	465	1	158	107	8	0	22	78	3	1	101	8	123	26	68	37	72	5	105
2000	528	2	288	122	4	0	21	148	12	5	170	40	151	45	91	62	50	9	146
2001	305	1	175	61	1	4	23	63	0	1	86	20	66	25	18	38	21	12	71
Total	2,170	11	1,005	497	45	4	165	402	20	15	525	77	636	170	277	223	253	53	555
Washington																			
1996	257	0	182	35	3	0	21	63	1	3	8	7	56	23	10	7	10	1	49
1997	634	1	456	108	6	0	45	135	2	1	32	57	121	43	18	17	9	6	89
1998	791	0	532	129	8	0	146	304	3	3	26	72	112	38	23	10	17	9	77
1999	1,172	1	903	121	6	0	16	537	1	0	32	22	89	59	15	21	19	55	103
2000	1,582	2	826	90	12	2	20	318	25	3	12	28	135	76	22	30	15	16	135
2001	686	1	351	69	2	1	26	153	12	1	14	31	65	34	22	11	10	4	74
Total	5,122	5	3,250	552	37	3	274	1,510	44	11	124	217	578	273	110	96	80	91	527

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
West Virginia																			
1996	12	2	9	9	2	0	8	6	1	1	15	0	15	4	2	0	3	0	23
1997	22	3	16	18	5	0	7	0	3	0	4	2	20	1	7	0	5	1	35
1998	24	0	18	18	4	0	3	7	0	1	13	2	24	6	12	0	14	2	28
1999	24	0	16	13	4	0	3	3	0	0	4	2	28	5	4	2	7	0	23
2000	31	0	16	9	5	0	8	7	1	0	6	1	22	4	7	1	13	1	14
2001	21	0	6	3	1	0	4	2	0	0	3	2	8	0	1	0	3	0	6
Total	134	5	81	70	21	0	33	25	5	2	45	9	117	20	33	3	45	4	129
Wisconsin																			
1996	97	1	62	20	9	0	4	7	0	1	0	2	43	8	12	2	15	1	37
1997	177	1	64	43	12	0	3	13	0	1	7	5	61	13	14	7	23	1	41
1998	245	1	80	43	19	0	9	22	0	1	17	4	79	15	15	1	14	2	49
1999	284	0	92	49	8	0	12	41	0	2	25	8	81	5	23	8	20	4	61
2000	319	1	143	47	15	2	13	48	3	5	12	9	97	15	28	9	41	12	69
2001	167	0	77	29	3	1	12	31	1	5	13	2	45	12	10	3	15	5	48
Total	1,289	4	518	231	66	3	53	162	4	15	74	30	406	68	102	30	128	25	305

State/Territory	Violation																		
	BSA/Structuring/Money Laundering	Bribery/Gratuity	Check Fraud	Check Kiting	Commercial Loan Fraud	Computer Intrusion	Consumer Loan Fraud	Counterfeit Check	Counterfeit Credit/Debit Card	Counterfeit Instrument (Other)	Credit Card Fraud	Debit Card Fraud	Defalcation/Embezzlement	False Statement	Misuse of Position or Self Dealing	Mortgage Loan Fraud	Mysterious Disappearance	Wire Transfer Fraud	Other
Wyoming																			
1996	5	0	3	1	1	0	1	0	0	0	0	0	6	1	1	0	0	0	2
1997	6	0	4	1	0	0	0	2	0	0	4	1	2	0	0	0	1	0	2
1998	15	0	6	5	3	0	0	0	1	0	3	0	2	2	0	0	0	0	5
1999	9	0	6	3	2	0	0	0	0	0	1	0	5	1	1	0	0	1	4
2000	21	0	2	4	1	0	1	2	0	0	0	0	10	1	4	1	3	0	4
2001	11	0	7	7	3	0	1	0	0	0	60	0	2	5	3	0	3	0	3
Total	67	0	28	21	10	0	3	4	1	0	68	1	27	10	9	1	7	1	20