Identity Theft

Trends, Patterns, and Typologies Based on Suspicious Activity Reports

Filed by the Securities and Futures Industries
January 1, 2005 – December 31, 2010

September 2011

Identity Theft

Trends, Patterns, and Typologies Based on Suspicious Activity Reports

Filed by the Securities and Futures Industries
January 1, 2005 – December 31, 2010

September 2011

Table of Contents

INTRODUCTION

This report focuses on identity theft in the securities and futures industries. Based on Suspicious Activity Report by the Securities and Futures Industries (SAR-SF) filings, it describes recent patterns and trends of SAR-SF reporting and identifies methods by which identity thieves may access and abuse investment, retirement, and trust accounts to defraud individual account holders and/or securities firms.

FinCEN added identity theft as a characterization of suspicious activity on the SAR-SF form in May 2004 following an increase in the reporting of this type of activity. This study is based on SAR-SF filings made between 2005 and 2010. It complements an October 2010 FinCEN report that described, in part, ways that identity thieves reportedly defraud individuals and depository institutions by gaining unauthorized access to credit cards, loans, and depository accounts.[1]

1. See *Identity Theft –Trends, Patterns, and Typologies Reported in Suspicious Activity Reports Filed by Depository Institutions, October 2010*, available at http://www.fincen.gov/news_room/rp/reports/pdf/ID%20Theft.pdf.

EXECUTIVE SUMMARY

- The number of SAR-SFs reporting identity theft grew by 89 percent from 2005 to 2010, and nearly 13 percent of all SAR-SF filings over the 6-year period in part characterized the reported activity as identity theft.[2] However, because the number of all SAR-SF filings grew by over 170 percent during the same period, the proportion of all SAR-SFs referencing identity theft declined from about 15 percent in 2005 to somewhat less than 10.5 percent in 2010.
- Over 86 percent of SAR-SF filings that either characterized identity theft or mentioned identity theft in the narrative section described apparent identity theft. Most of the remainder of sample filings described possible identity theft, but absent contact with the apparent victim could not be considered as such.[3]
- Wire fraud, virtually always described as Automated Clearing House (ACH) fraud, was the suspicious activity characterization most frequently co-reported with identity theft, appearing in nearly 53 percent of the relevant sample filings.[4] Over 31 percent of filings reported that unauthorized ACH transfers were used to shift funds from victim investment accounts to depository accounts controlled by thieves. Just over 24 percent of filings reported thieves used unauthorized ACH transfers to move money from victim depository accounts to unauthorized new investment accounts the thieves set up using stolen identifiers.
- Identity thieves reportedly employed computer intrusion in over 39 percent of sample filings to both facilitate collection of victim identifiers and to initiate unauthorized transactions. However, reporting of computer intrusion declined steeply after the second quarter of 2008.
- Although the general public's use of checks is declining, identity thieves used checks to promote financial fraud in nearly 16 percent of sample filings, and the trend in reports of thieves' check use increased modestly. Just over 6 percent of filings reported identity thieves used debit cards to steal funds, and both debit card usage and dollar loss trends moved strongly up.

2. FinCEN read a random sample of identity theft associated SAR-SF filings submitted between January 1, 2005, and December 31, 2010.
3. This report uses the term "victim" to describe an individual whose identity was stolen, whether or not the thief ultimately benefitted from using the identifiers. "Victims" and their financial institutions may both suffer losses from financial fraud facilitated by the stolen identifiers.
4. Each SAR-SF filing may report multiple suspicious activity characterizations.

- The main thrust of financial fraud associated with investment accounts was the direct theft of funds from victim accounts. Nonetheless, between the fourth quarter of 2006 and the first quarter of 2008, 20-40 percent of quarterly filings reported thieves attempting to manipulate the share values of thinly-traded securities with funds stolen from the investment and/or depository accounts of identity theft victims.
- Quarterly sample data highlights the thieves' growing success rate in the direct theft of funds from victim accounts; data associated with unauthorized trading in victim investment accounts indicates generally successful outcomes over the whole study period.
- About 90 percent of study filings reported the abuse of an existing legitimate investment account or the unauthorized set up of a new investment account using stolen identifiers. Most affected investment accounts referenced in the sample were standard individual accounts. However, over 16 percent of filings reported one or more affected retirement accounts, and over 2 percent reported affected individual or family trust accounts. Reporting trends associated with both retirement and trust accounts were up markedly.
- During most of the 2005-2010 study period, identity thieves reportedly showed a preference for taking over existing legitimate investment accounts rather than setting up new unauthorized accounts using stolen identifiers. This preference appears to relate to the greater level of scrutiny investment firms place on new accounts compared to the level they place on existing accounts.
- Study findings identified novel typologies thieves use to commit fraud. These include use of Voice-over-Internet-Protocol phone numbers and telephone relay services to mask their identities; use of stolen credit card numbers to temporarily fund day trading and quick re-crediting of the charge account with a portion of the trading profits to hide the original theft; abuse of legitimate corporation names to set up and drain unauthorized accounts funded with legitimate checks stolen from the mail; hacking of state sex offender registries and use of offenders' identifiers to set up unauthorized accounts; use of university student identifiers to open investment accounts to evade taxes on investment earnings; use of hundreds of sets of stolen identifiers to abuse investment company promotional account features such as ATM fee refunds and cash bonuses for opening new accounts; and feigning identity theft to defraud financial institutions that made their accounts whole following purportedly unauthorized transactions the account holders actually initiated themselves.

METHODOLOGY

For this study, FinCEN defined identity theft as using identifying information unique to the rightful owner without the rightful owner's permission. Unique identifying information includes financial account numbers, such as those used for depository accounts, investments, loans, credit cards, or online payment accounts; officially-issued federal or state identifying documents; and biometric information. An individual's use of another person's Social Security Number (SSN) or Individual Tax Identification Number (ITIN) was considered identity theft regardless of whether the individual knew whether, or to whom, the number was issued. Additionally, impersonation of an actual person without consent was considered identity theft regardless of whether the impersonation occurred in person or through any other medium, electronic or otherwise.

In identifying potential trends, FinCEN reached out to representatives of the Bank Secrecy Act Advisory Group (BSAAG)[5] Securities and Futures Subcommittee for input as to the types of information industry would find most useful in this report.

FinCEN analysts conducted database research to identify SAR-SF filings made between January 1, 2005 and December 31, 2010, in which filers checked the box specifying identity theft as a characterization of suspicious activity. Analysts added a small number of filings to the study population that specifically mentioned identity theft in the SAR-SF narrative but did not characterize the activity as identity theft by inclusion of a check mark on the form.

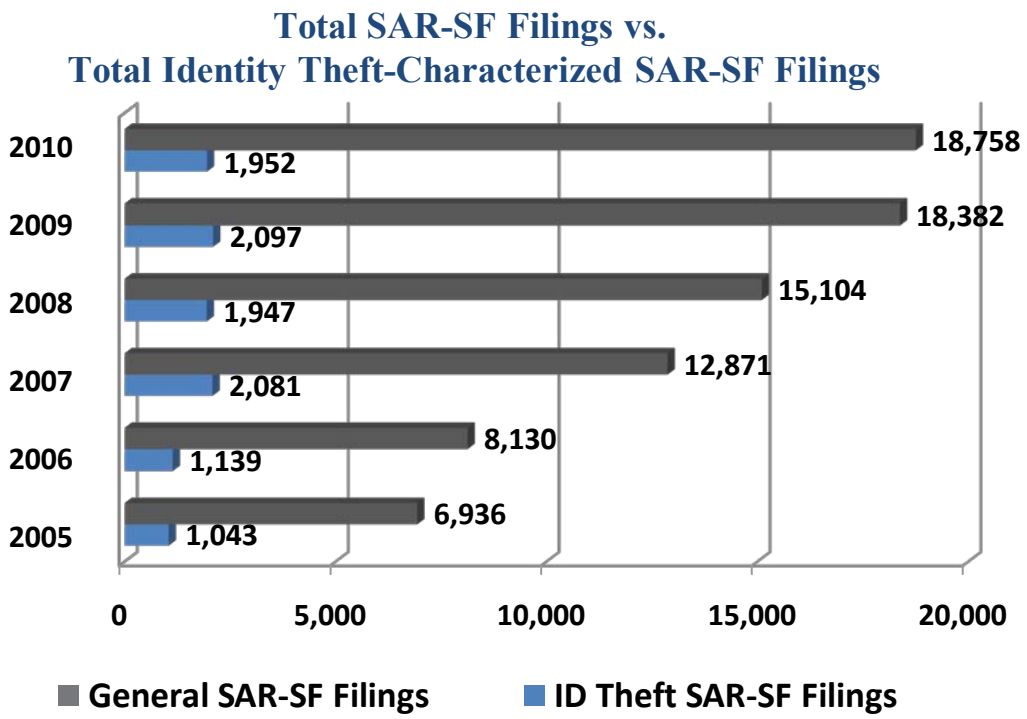
Unless otherwise noted, findings were based upon the weighted combination of data results from two studies–the first analyzing a random sample of filings received between January 1, 2005 and September 30, 2008, and the second analyzing a random sample of filings received between October 1, 2008 and December 31, 2010.[6] References throughout the report to "relevant sample filings" refer to the approximately 86 percent of the sample filings that analysis determined describe apparent identity theft.

5. The Annunzio-Wylie Anti-Money Laundering Act of 1992 required the Secretary of the Treasury to establish the Bank Secrecy Act Advisory Group ("BSAAG") as a forum for the financial services industry, law enforcement and regulators to advise the Secretary on ways to enhance the usefulness of Bank Secrecy Act ("BSA") reporting. Since 1994, the BSAAG has served as a forum for these groups to discuss the uses of Suspicious Activity Reports, Currency Transaction Reports, and other BSA reports, and how recordkeeping and reporting requirements can be improved. The BSAAG utilizes a variety of permanent and ad hoc subcommittees to identify and analyze relevant issues.
6. Weighting was determined based on the percentage of the whole identity theft-characterized filing population each study sample represented.

GENERAL STATISTICS

Graph 1 demonstrates that though the number of identity theft-characterized SAR-SF filings grew significantly from 2005-2007, the numbers of such filings have remained generally stable since. Conversely, the overall number of SAR-SF filings grew markedly during 2005-2009, and then modestly from 2009-2010. Consequently, SAR-SF filings characterizing identity theft represented about 15 percent of all SAR-SF filings in 2005, but just less than 10.5 percent in 2010.

GRAPH 1



FinCEN determined that approximately 86 percent of sample filings described identity theft. Most of the rest of the filings may also have described identity theft, though absent contact with the apparent victim, the filer could not determine whether the reported activities signaled identity theft or customer attempts to commit fraud.

ACTORS

Filers

Incidence

The 1,395 sample filings that described identity theft were submitted by 160 distinct filers. The five most prolific filers accounted for approximately 58.5 percent of these filings, while the top 10 filers accounted for nearly 70.5 percent.

Geography

Filer addresses spanned 27 states. Chart 1 provides a breakdown showing the approximate percentage of the 160 distinct filers by state.[7]

CHART 1

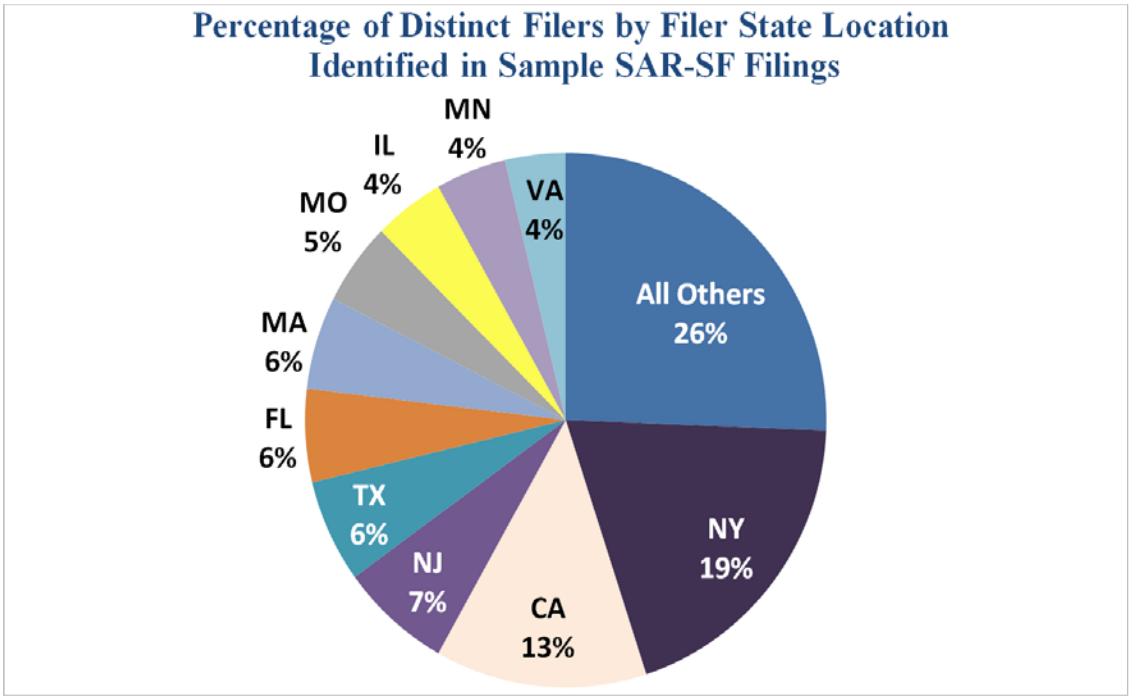
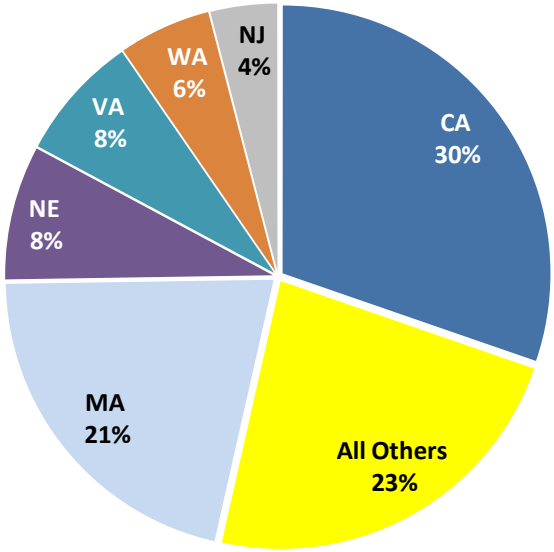


Chart 2 indicates that together filer branch locations in California, Massachusetts, Nebraska, Virginia, Washington, and New Jersey submitted about 77 percent of the relevant sample filings.

7. Chart 1 is based on the headquarters address of each distinct filer represented in the study sample.

CHART 2

Percentage of Total Sample Filings by Filer Branch State Location



Business Activities

Table 1 displays how the 160 distinct filers identified their institution type(s).[8] As the table shows, introducing brokers made up the highest proportion of filers.

TABLE 1

INSTITUTION TYPE	*INCIDENCE OF DISTINCT FILERS REPORTING*	*PERCENTAGE OF TOTAL DISTINCT FILERS*
Securities Broker - Introducing	67	41.88%
Securities Broker - Clearing	35	21.88%
Securities Dealer	31	19.38%
Investment Company – Mutual Fund	26	16.25%
Other	19	11.88%
Affiliate of Bank Holding Company	15	9.38%
Investment Adviser	11	6.88%
Subsidiary of Bank	8	5.00%
Futures Commission Merchant	7	4.38%
LEFT BLANK	7	4.38%
Market Maker	7	4.38%

8. Most filers chose multiple institution types to describe their various business activities.

INSTITUTION TYPE	*INCIDENCE OF DISTINCT FILERS REPORTING*	*PERCENTAGE OF TOTAL DISTINCT FILERS*
Securities Options Broker-Dealer	4	2.50%
Municipal Securities Dealer	3	1.88%
Agricultural Trade Option Merchant	2	1.25%
Securities Floor Broker	2	1.25%
U.S. Government Broker-Dealer	2	1.25%
Direct Participation Program	1	<1%
Introducing Broker - Commodities	1	<1%

Table 2 ranks these institution types based upon the number of relevant sample filings reporting them.

TABLE 2

INSTITUTION TYPE	*INCIDENCE OF SAMPLE FILINGS*	*PERCENTAGE OF TOTAL SAMPLE FILINGS*
Securities Broker - Clearing	661	47.38%
Securities Broker - Introducing	531	38.06%
Other	448	32.11%
Affiliate of Bank Holding Company	376	26.95%
Investment Company – Mutual Fund	263	18.85%
Securities Dealer	243	17.42%
Investment Adviser	157	11.25%
Market Maker	145	10.39%
Subsidiary of Bank	71	5.09%
LEFT BLANK	24	1.72%
Futures Commission Merchant	17	1.22%
Securities Options Broker-Dealer	15	1.08%
Municipal Securities Dealer	8	<1%
Agricultural Trade Option Merchant	5	<1%
Introducing Broker – Commodities	5	<1%
Securities Floor Broker	3	<1%
U.S. Government Broker-Dealer	3	<1%
Direct Participation Program	1	<1%

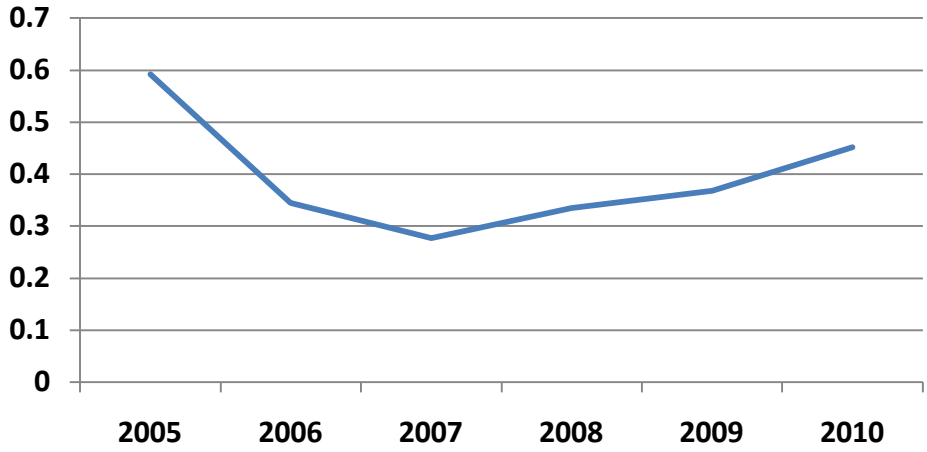
Subjects

Incidence & Geography

Graph 2 highlights the paucity of subjects reported within the whole population of SAR-SF filings submitted between 2005 and 2010 that characterize identity theft.

GRAPH 2

Average Subjects Reported per Identity Theft-Characterized SAR-SF Filing by Year



To place these numbers in context, depository institution SAR filers reported an average of nearly one subject per SAR filing in the aforementioned October 2010 study. The average for SAR-SF filers is almost certainly much lower because most investment transactions, whether legitimate or otherwise, are initiated and completed online or by phone, fax, or mail and rarely involve face-to-face contact with investment industry employees. In contrast, depository institution branch personnel are more likely to experience periodic face-to-face contact with the majority of their branch customers and other individuals intending to complete financial transactions.[9]

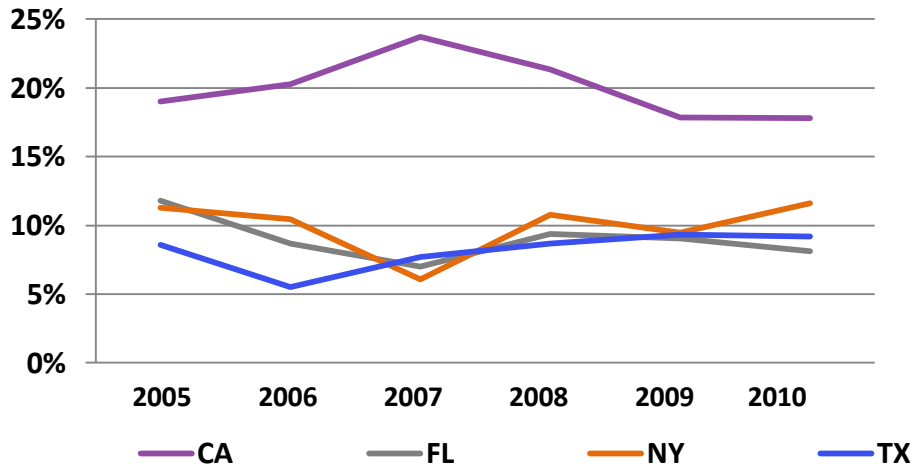
9. The shape of the line in Graph 2 also appears to correlate with data presented later in the report comparing the effects of the apparently shifting focus of thieves from the direct theft of funds in the earliest data, toward market manipulation in the mid study years, and back toward direct theft in the newest data. Logically, a greater proportion of filings reporting market manipulation would contribute to a lower number of identifiable subjects since the thief who is attempting market manipulation is not generally moving money into or out of victimized accounts, and is thus not providing any identifier such as account number or physical address to which stolen funds are to be sent.

Analysis of the whole population of identity theft characterized SAR-SF filings submitted between 2005 and 2010 identified 3,506 individual and 55 business subjects. Though most of these were unique, filers reported about 2.5 percent of the individual subjects in multiple filings.[10] Multiple institutions submitted filings on the majority of these individuals.

Graph 3 highlights the continued predominance of California as the most frequently reported state of subject residence. Florida, New York, and Texas have traded places for ranks 2 through 4 over the course of the study period.

GRAPH 3

Most Frequently Reported Subject Residence States as an Annual Percentage of All Identity Theft-Characterized SAR-SF Filings



With respect to the most recent data, analysis of the whole population of 2010 SAR-SF filings bearing the identity theft characterization (1,952 filings) identified 813 distinct subjects with residences in the United States. Of these subjects, 32 were businesses.[11]

10. Filers reported most of these recurring subjects in different years at the same or similar address. Filers reported about 15 percent of this subject subset resident in multiple and sometimes geographically dispersed states.

11. FinCEN included the 50 states, plus the District of Columbia, Puerto Rico, and the Virgin Islands as the covered jurisdictions in the total subject and total population calculations. Data displayed in the tables was limited to the 50 states. Of the total 1,952 filings analyzed, 880 reported no subject names at all, while another 374 reported characters in the subject name fields intended to convey no subject names were known. Consequently, only 698 (just under 36 percent) of the 1,952 filings reported any valid subject names.

Table 3 displays the top 10 subject residence states. As would be expected, the majority of reported subjects resided in the more populous states.

TABLE 3

STATE	NUMBER OF DISTINCT ID THEFT SUBJECTS BY ZIP CODE	PERCENT OF TOTAL SUBJECTS
California	145	17.84%
New York	94	11.56%
Texas	76	9.35%
Florida	64	7.87%
Michigan	34	4.18%
Illinois	30	3.69%
New Jersey	26	3.20%
Virginia	23	2.83%
Georgia	22	2.71%
Massachusetts	21	2.58%
TOTAL	535	65.81%

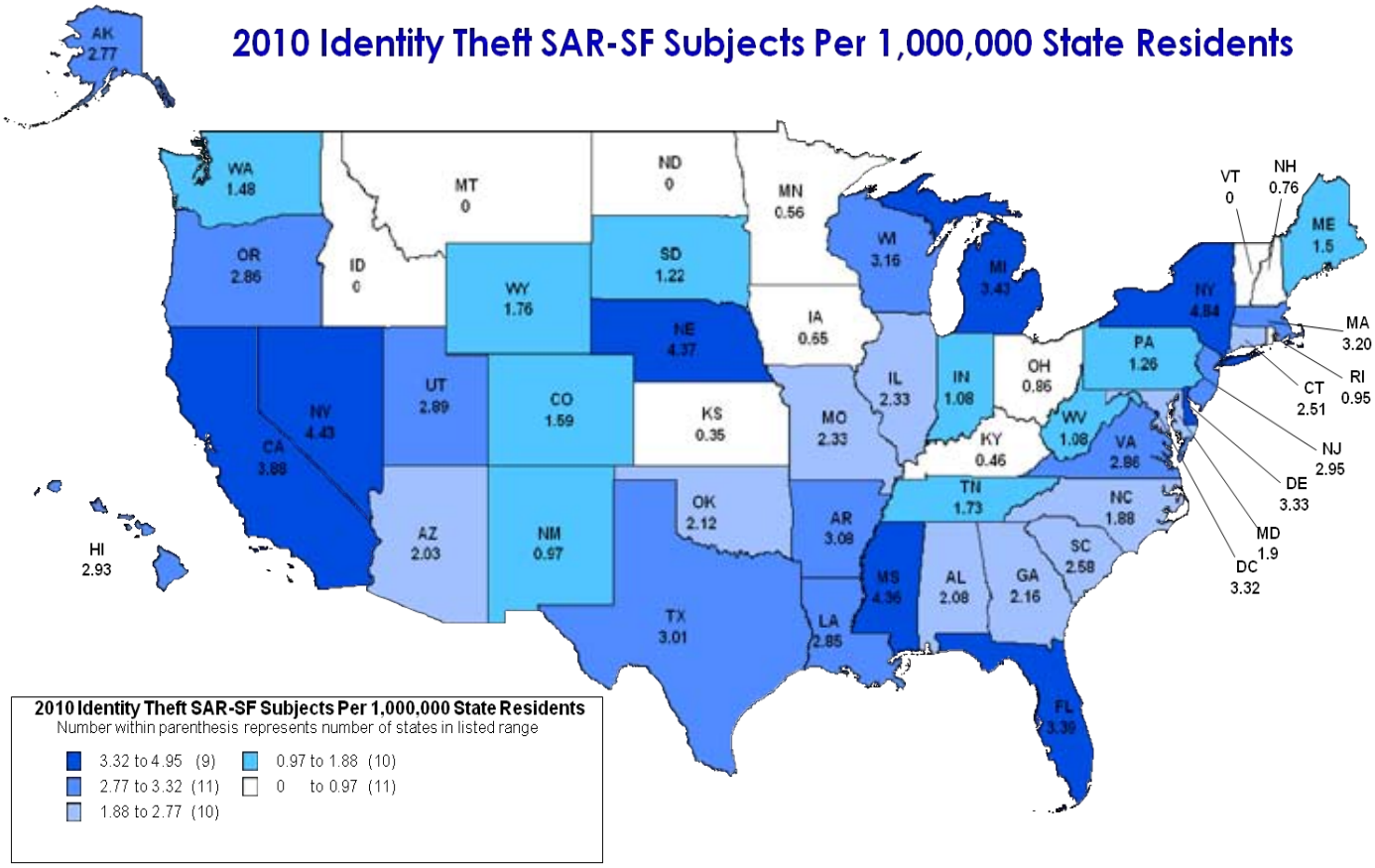
Table 4 displays the top 10 states with the highest number of reported identity theft subjects per million state residents.

TABLE 4

RANK	STATE	2010 SAR-SF IDENTITY THEFT SUBJECTS REPORTED PER MILLION RESIDENTS
1	New York	4.84
2	Nevada	4.43
3	Nebraska	4.37
4	Mississippi	4.36
5	California	3.88
7	Michigan	3.43
6	Florida	3.39
9	Delaware	3.33
8	Massachusetts	3.20
10	Wisconsin	3.16

Map 1 displays the incidence of identity theft subjects in 2010 per million state residents.[12]

MAP 1



Analysis identified an additional 68 subjects, including 7 businesses, located outside the United States. Prominent subject residence countries included the United Kingdom (16), Nigeria (9), Venezuela (8), Uganda (5), and South Africa (5).

12. Analysis of the filings for Nebraska and Mississippi indicated that there were relatively few filings, but that each uncharacteristically reported between 3 to 5 subjects. This explains the large proportional numbers reported for two states with comparatively small populations.

Subject Intent and Relationship to Victim

Analysis of the overall sample indicated nearly 94 percent of filings described activity where the subject clearly intended to defraud either the identity theft victim or the filer. Somewhat less than 5 percent of the sample described subjects who apparently used stolen identifiers to secure employment. The remaining approximate 1.5 percent of filings did not describe any clear motive for use of the victim's identifiers.

According to almost 7 percent of relevant sample filings, the victim reportedly knew the presumed identity thief. The reporting trend showed a marked increase from about 5 percent in 2005-2008 to over 8 percent of filings in 2009-2010.

FinCEN located few sample filings reporting criminal involvement of current or former filer employees. Overall, about one half percent of filings reported such activity. Filers did report an upswing in the number of instances in which individuals impersonated filer employees (just over one half percent of filings) with all but one such report appearing in the 2009-2010 sample.

Victims

Because Bank Secrecy Act (BSA) form instructions do not require the filer to provide specific information on victims, victims are often not a focus of such filings. Consequently, the sample SAR-SF filings provide only fragmentary information about victims. In some cases, the filer was unable to contact the apparent victim and was thus unable to determine whether that individual was actually a victim or was instead involved in an attempt to defraud the filer.

Nonetheless, analysis indicated that about 2.5 percent of sample filings reported that the target of identity theft was deceased at the time the identity theft occurred. Somewhat over 1.5 percent reported that the thief engaged in elder financial exploitation as part of the alleged crime.[13]

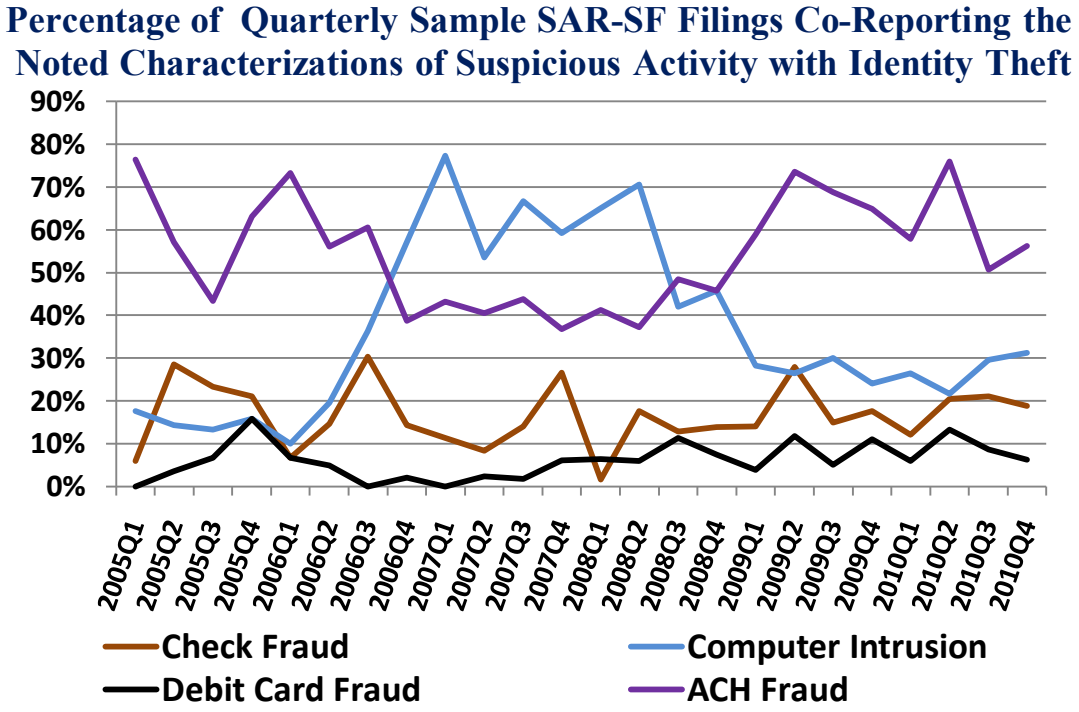
13. See http://www.fincen.gov/statutes_regs/guidance/html/fin-2011-a003.html.

TYPOLOGIES, TRENDS, AND PATTERNS

Co-Reported Characterizations of Suspicious Activity

Identity thieves steal victim information by various methods and for a variety of reasons, primarily to facilitate various types of financial fraud. Graph 4 displays the quarterly percentages of sample filings also reporting ACH fraud, computer intrusion, check fraud, and debit card fraud, the characterizations of suspicious activity most frequently co-reported with identity theft.[14]

GRAPH 4



14. The analyst derived this data through narrative analysis and reported the noted characterizations regardless of whether the attempted activity proved successful or not. Many sample filings described the identity thief's use of multiple payment vehicles to facilitate the theft of victim funds.

ACH Fraud

ACH fraud was the identity thief's preferred method to transfer and aggregate stolen funds over the entire study period.[15] The median attempted amount of ACH fraud increased from $20,950 in 2005-2008 to $26,500 in 2009-2010. However, the median loss amount associated with these attempts changed very little: median reported loss was $13,998 in 2005-2008 and $14,060 in 2009-2010. Overall, about 24 percent of sample filings reported identity thieves illicitly drawing funds from depository accounts using ACH to fund existing investment accounts they had taken over or new accounts they had set up. The trend line for this type of activity was moderately up. Somewhat more than 30.5 percent of filings reported thieves using ACH to move funds out of victimized investment accounts and into thief-controlled depository accounts, with the trend line for this activity increasing more steeply. Thieves reportedly also used ACH to move funds from one investment account to another in 5.5 percent of filings, with the trend up steeply.

Computer Intrusion

From the first quarter of 2006 through the second quarter of 2008, computer intrusion became a primary reported means by which identity thieves gathered victim identifiers and financial account information. Suspected thieves reportedly used this information to initiate unauthorized financial transactions both within legitimate existing victim accounts and within unauthorized accounts they set up using stolen identifiers. Though the sharp drop off in reported computer intrusion thereafter may suggest that filers and their customers have had some success in fending off computer intrusion using various cyber countermeasures, some of the drop off may also suggest that identity thieves are employing more sophisticated forms of computer intrusion, less likely to be detected and reported as the means of identity theft.[16]

Check Fraud

Although 2010 Federal Reserve Payments Study data report the public's usage of checks declining in comparison to most other payment methods, identity thieves continue to find checks a useful vehicle to facilitate financial fraud.[17] The median

15. Virtually every sample SAR-SF that co-reported the characterization "wire fraud" involved ACH rather than traditional wire transfers.
16. One countermeasure that appears to have provided significant protection is filer provision of tokens to their clients that generate new random account passwords each minute.
17. See http://www.frbservices.org/files/communications/pdf/research/2010_payments_study.pdf, page 11.

amount of attempted check fraud-related activity was $12,900 in 2005-2008, but jumped to $33,865 in 2009-2010. The median loss amount jumped as well, from $9,065 in the earlier period to $21,000 in 2009-2010. In somewhat more than 3.5 percent of sample filings, thieves reportedly used second party checks drawn on depository accounts without authorization to fund investment accounts (trend was moderately increasing), and third party checks in just over 2 percent of sample filings (trend was moderately up).

Thieves frequently used checks to drain investment accounts. They reportedly used checks drawn directly upon victim investment accounts or upon linked demand accounts in about 5 percent of filings (trend was sharply up), or requested checks drawn on the investment firm's official disbursement account in almost 7 percent of filings (trend was modestly down).

Debit Card Fraud

Identity thieves have increased their use of debit cards to steal victim funds. Though overall attempted debit card fraud and loss amounts were lower than those associated with ACH fraud or check fraud, filers generally lost the full amount of unauthorized debit card transactions. On the other hand, filers could often stop unauthorized check or ACH transactions, resulting in a full or partial recovery of funds. Study findings indicated that median unauthorized debit card transactions attempted and resulting losses were both $6,309 in 2005-2008 and increased to $13,408 in 2009-2010 (trend was up sharply).

Other Characterizations of Suspicious Activity

Filers characterized identity-theft related activities as securities fraud in nearly 25.5 percent of the relevant sample filings. Most filings appear to have characterized securities fraud based upon reported attempts to engage in market manipulation through the purchase or sale of large blocks of thinly-traded securities.[18] Since securities fraud can be defined broadly, FinCEN chose to specifically address the types of activities most frequently reported in SAR-SFs that comprise securities fraud rather than to generally characterize them as securities fraud.

18. See the Federal Bureau of Investigation's definition of securities fraud at http://www2.fbi.gov/publications/fraud/securities_fraud.htm. See also the U.S. Securities and Exchange Commission's Guide to Identifying and Avoiding Securities Fraud at http://www.sec.gov/investor/pubs/identavoidfraud.htm.

Filers reported other characterizations of suspicious activity in much lower numbers. In virtually all instances, FinCEN narrative analysis located larger numbers of filings characterizing any given activity captured on the SAR-SF than the filers recorded. One exception was structuring/money laundering, which filers characterized in nearly 3 percent of the overall sample. FinCEN characterized structuring/money laundering only when it appeared to be an intentional part of the reported activities and estimated it on that basis at somewhat less than 1.5 percent of the filings.

Account Abuse Scenarios

Filers recounted several common account abuse scenarios in the study sample. The most common scenario involved the abuse of one or more existing victim accounts. The thief generally used account access information collected through a variety of methods including computer intrusion, physical theft from the victim's home or vehicle, theft of the victim's mail or trash, phishing, and vishing.[19] The thief generally accessed accounts through online banking or investment services and frequently also communicated by means of phone or fax. After accessing the account, the thief would often change contact information such as physical and email addresses, phone numbers, and online access passwords. In many instances, the thief directed that cash balances in an investment account be sent by ACH to another account controlled by the thief or mailed by check to the new address the thief placed on the account. In instances where the thief found the account balances in the form of securities, the thief would often order that these positions be liquidated and the proceeds sent by ACH to his account or by check to his address. In some instances where the thief knew the target had an account at the filing institution, but did not have sufficient access information to enter the account, the thief attempted to use social engineering (vishing) to persuade a filer employee or the target to provide the missing account access information.

19. Phishing and vishing both involve social engineering but rely on different technology. In vishing, the thief contacts the target by phone, usually by Voice-over-Internet Protocol (VoIP) so that the call can't be traced, and misrepresents himself as someone entitled to gather personal identifiers, such as a financial institution employee, a law enforcement or tax authority representative, or a medical services provider employee. Within the study sample, those employing vishing generally identified themselves as employees of a financial institution where the target maintained one or more accounts. Phishing is accomplished online rather than by phone. Like vishers, phishers frequently pose as representatives of the target's financial institution, employing email and links to a spoofed financial institution Web site in attempts to gather personal information.

Another common scenario involved thieves who did not have account access information, but did have stolen identifiers. Identity thieves often used this information to open one or more new unauthorized accounts in the victim's name. The thief most frequently used the new account to receive unauthorized ACH transfers or fraudulent/counterfeit checks from other investment accounts or from depository accounts. As soon as these funds hit the new account, the thief generally attempted to move the money out of the account to other accounts the thief controlled. The thief most frequently moved funds using unauthorized ACH transfers, but also wrote checks against the account or used the ATM/debit card issued at account opening to drain cash or make online or point-of-sale purchases before the financial institution received notice that the funding ACH or check was unauthorized or fraudulent.

Less commonly, the thief opened an account, funded it as noted and immediately attempted to use the funds to purchase securities, quickly selling these and moving the money out of the account as above. In most instances the purchase of securities was designed to make the investment account appear legitimate. In other cases, the thief may have hoped to profit further from the purchase and sale of these securities.

In a fourth scenario, the thief used existing victim account balances or funds fraudulently deposited into a new unauthorized account for the clear purpose of market manipulation. In this scenario, the thief used account balances to purchase large blocks of thinly-traded securities in order to drive up the share value. Immediately after these purchases, the thief sold large blocks of the same security he held in other accounts, thus reaping a quick profit.

Though the sample filings generally described the abuse of investment accounts, many filers were not able to establish whether a new or existing customer account was being abused by an identity thief or, alternately, by the actual customer engaging in financial fraud. Often, the filer could establish identity theft only by verifying that the owner of the account used to fund a new or existing investment account did not authorize the ACH debit or check drawn against the funding account.

Investment Account Abuse

Direct Theft of Funds

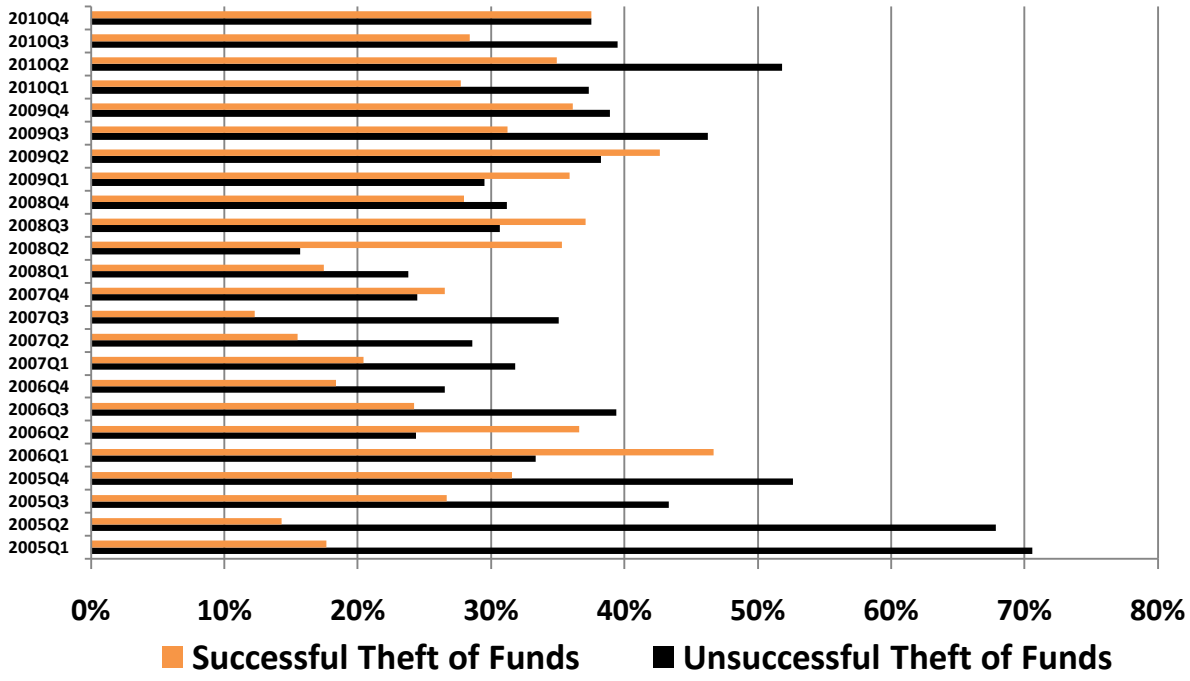
About 90 percent of study filings reported the abuse of an existing legitimate investment account or the unauthorized set up of a new investment account using stolen identifiers. The trend in investment account abuse reporting was slightly down over the period of the study.

Identity thieves most frequently abused victim investment accounts by directly stealing funds from these accounts.

Graph 5 shows the quarterly percentages of sample filings reporting successful and unsuccessful thefts of funds from all types of victim accounts.

GRAPH 5

Percentage of Quarterly Sample Filings Reporting Successful and Unsuccessful Thefts of Funds from all Types of Victimized Accounts



Overall, the graph demonstrates an increase in the identity thief's success rate in stealing funds directly from both victim investment and depository accounts, using all of the payment vehicles noted in Graph 4, plus, much less frequently, others such as counterfeit checks (somewhat more than 1.5 percent of filings) and prepaid access (about one half percent of filings).[20] Filers also reported the identity thief's attempts to abuse the loan features of some investment accounts (somewhat more than 1 percent of filings), and to use investment accounts in association with mortgage loan fraud (about one half percent of filings).

20. In each reported instance, the prepaid access device was a card.

Table 5 displays average and median dollar amounts of filer-reported financial fraud and the associated losses that did not involve trading activity, mainly involving ACH fraud, check fraud, and/or debit card fraud.

TABLE 5

	2005-2008 Activity Amount	***2005-2008 Associated Loss***	***2009-2010 Activity Amount***	***2009-2010 Associated Loss***
Average	$486,810	$41,740	$118,105	$102,661
Median	$24,664	$12,511	$23,315	$12,491

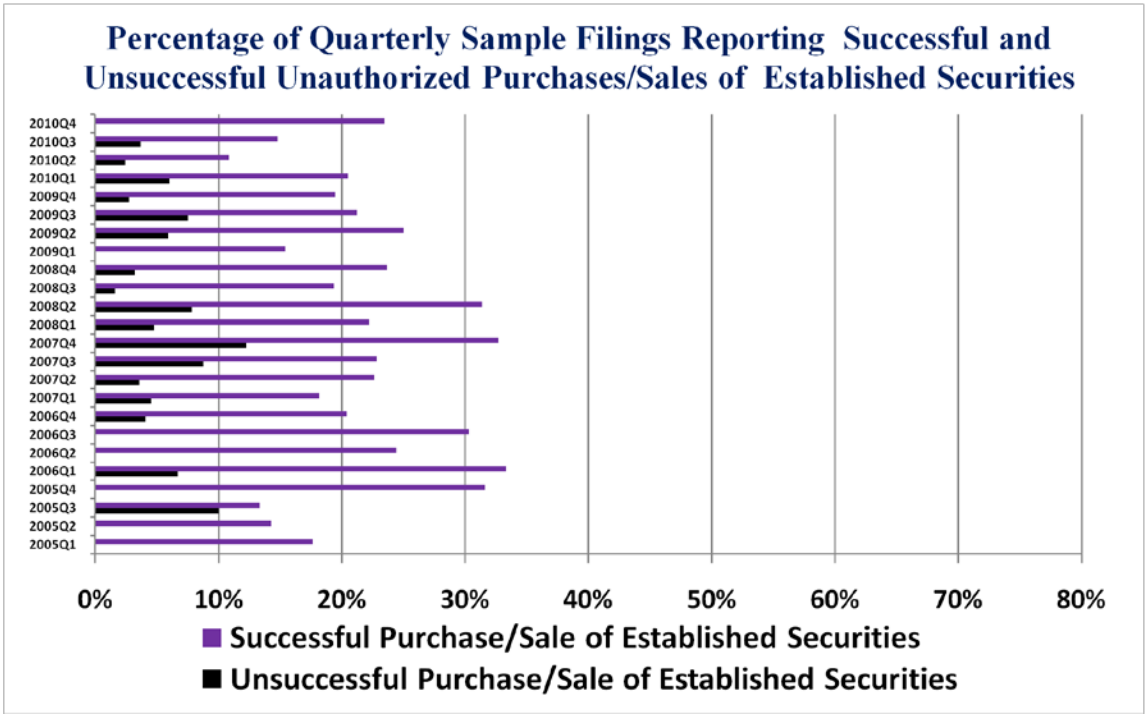
The average reported activity and associated loss amounts were extremely divergent between the earlier and later studies, showing a very large decrease in the average activity amount but a very large increase in the average associated loss amount. Conversely, the median activity and loss amounts reported in the two studies were notably similar.

Securities Trades

Generally, many investment accounts do not maintain significant cash balances, but frequently instead hold securities. Consequently, the thief who gains access to an existing investment account will often find the majority of account assets in a form other than cash. In these cases, the thief may initiate unauthorized sales of securities to liquidate the assets and make them easily transferrable to a depository account or to another investment account the identity thief controls.

Graph 6 provides study findings concerning the quarterly percentages of sample filings reporting successful and unsuccessful unauthorized purchases or sales of established securities.

GRAPH 6



Graph 6 clearly indicates that within the sample, identity thieves were generally successful in liquidating victim assets throughout the study period.

Some filings reported that rather than liquidate the victim's holdings, the thief transferred or attempted to transfer the victim's account intact employing the Automated Customer Account Transfer Service (ACATS) into an account the thief controlled at another brokerage or bank.[21] Just over 1 percent of sample filings reported the thief's attempted or successful use of ACATS. Though the majority of attempts were successful, the most recently reported attempts were not.

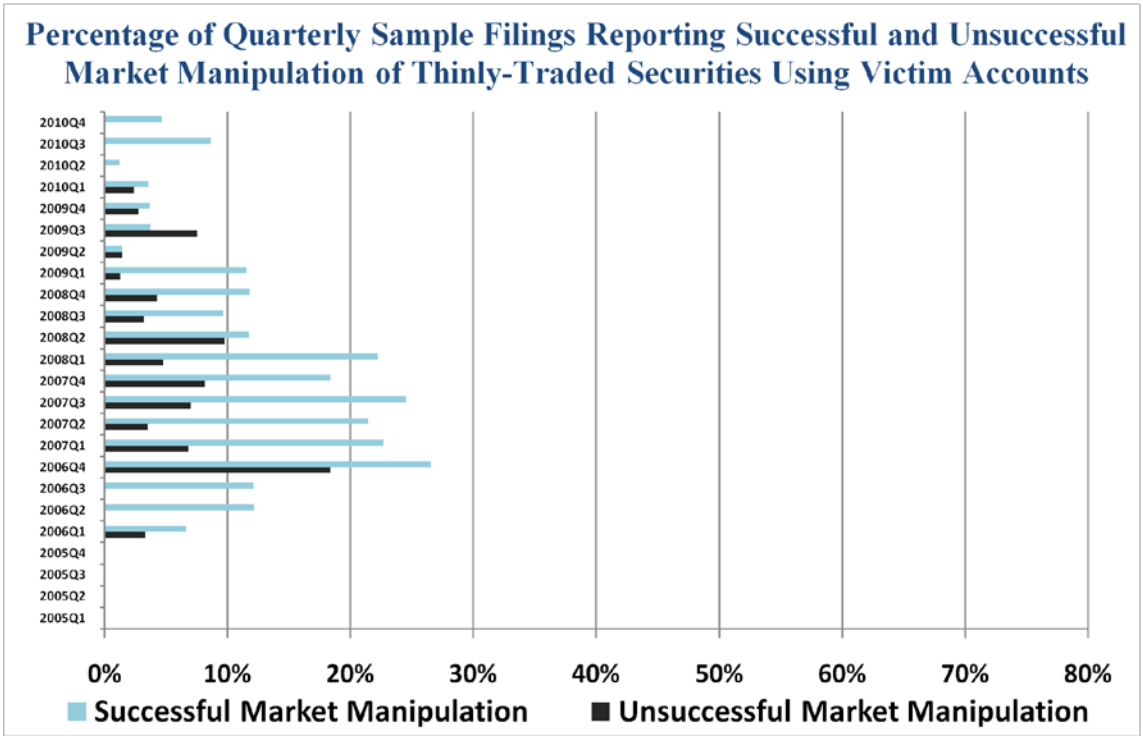
21. ACATS is a system that automates and standardizes procedures for the transfer of assets in a customer account from one brokerage firm and/or bank to another. The National Securities Clearing Corporation (NSCC), a subsidiary of the Depository Trust and Clearing Corporation (DTCC), developed the ACATS system. See http://www.dtcc.com/products/cs/equities_clearance/acats.php.

Market Manipulation

As noted previously, investment accounts provide the identity thief opportunities to defraud both account holders and the institutions that maintain investment accounts in ways not available to thieves targeting accounts maintained at depository institutions. More sophisticated or enterprising identity thieves may use victim investment accounts to manipulate the market in thinly-traded securities. In these cases, thieves may never actually steal money from a victim's account. Instead, thieves may use cash balances or liquidate securities holdings in an account to purchase shares in illiquid securities of companies that have very low market capitalizations, which may be more easily subject to market manipulation than other securities. Identity thieves generally already hold large positions in these securities in other investment accounts. As soon as they make large purchases in one or more victim account(s) to drive up the share price, they sell a large block of the same security held in other account(s) they control. In virtually all such cases, the victimized account holder is left with securities worth much less than the cash or more liquid securities held in the account prior to the fraudulent activity. Study findings recorded significant amounts of this type of activity. Graph 7 indicates the percentage of sample filings by quarter reporting successful and unsuccessful market manipulation.[22]

22. Successful market manipulation is defined for purposes of this study as thief-initiated trades in thinly-traded securities that filers fully or partially executed whether or not the effects of these trades moved share prices significantly.

GRAPH 7



Graph 7 indicates that within the study sample, the relative incidence of identity thieves' employment of market manipulation within victim accounts has dropped significantly since the highs reached from Quarter 4, 2006 through Quarter 1, 2008. Together, Graphs 5 and 7 show that the focus has shifted decisively back toward the direct theft of funds from victim accounts. This shift may have been at least partly associated with the instability seen in the markets following the banking crisis that began in September 2008.

A comparison of Graph 7 with Graph 4 also suggests a positive relationship between computer intrusion and market manipulation. The patterns and timeframes of both activities appear similar.

Since it is generally the policy of filers to make victimized customers whole, filers suffered significant losses restoring victimized investment accounts to their pre-fraud positions. Table 6 provides data concerning the average and median unauthorized trading amounts and associated filer losses reported in the study sample.[23]

TABLE 6

	2005-2008 Trading Amount	***2005-2008 Loss Incurred Restoring Victimized Account(s)***	***2009-2010 Trading Amount***	***2009-2010 Loss Incurred Restoring Victimized Account(s)***
Average	$157,001	$25,032	$438,013	$7,153
Median	$33,261	$2,000	$43,963	$674

Though average and median trading amounts increased significantly over the 6-year study period, reported associated average and median losses declined just as significantly.

23. Filers did not separately report their losses resulting from their liquidation of thinly-traded securities the thief purchased or related to their re-purchase of established securities the thief sold from victimized accounts. Loss amounts reported in Table 5 can be equated with the amount an identity thief was able to steal from the filer or another institution holding affected victim accounts. However, a thief 's enrichment cannot be gauged by the loss amounts reported in Table 6, which represent the amounts filers lost when they restored victimized customer accounts to their pre-fraud prevailing positions. Whether or to what extent the identity thief profited from the purchase or sale of securities in victim accounts depends upon whether attempts to manipulate the market in a given thinly-traded security in the victim's account succeeded; and whether the thief's sale of victim securities positions in established securities was followed by successful withdrawal of these liquidated funds through check or debit card transactions, or through a funds transfer to another account. Many filings reported the thief's successful sale of established securities in a victim account, but his failure to move these funds out of the victim's account prior to detection.

Instruments

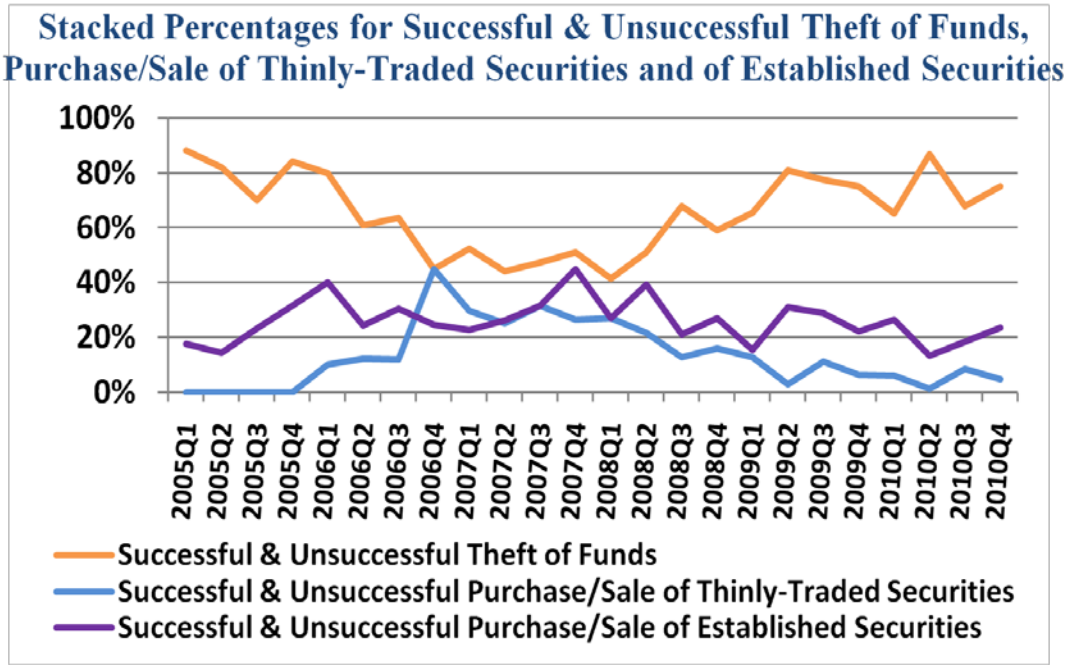
Table 7 displays a breakdown of the identifiable instrument types reported in all 488 filings referencing successful or unsuccessful unauthorized trading.

TABLE 7

INSTRUMENT	INCIDENCE	PERCENTAGE OF TOTAL IDENTIFIABLE INSTRUMENTS
Stocks	385	63.64%
Cash or Equivalent	161	26.61%
Mutual Fund	43	7.11%
Bonds/Notes	5	<1%
Money Market	4	<1%
Other Securities	3	<1%
Warrants	2	<1%
Commodity Type	1	<1%
Security Futures Product	1	<1%
TOTAL	605	100.00%

Graph 8 shows the relative incidence of reported successful and unsuccessful theft of funds, purchase/sale of established securities, and purchase/sale of thinly-traded securities by identity thieves.

GRAPH 8



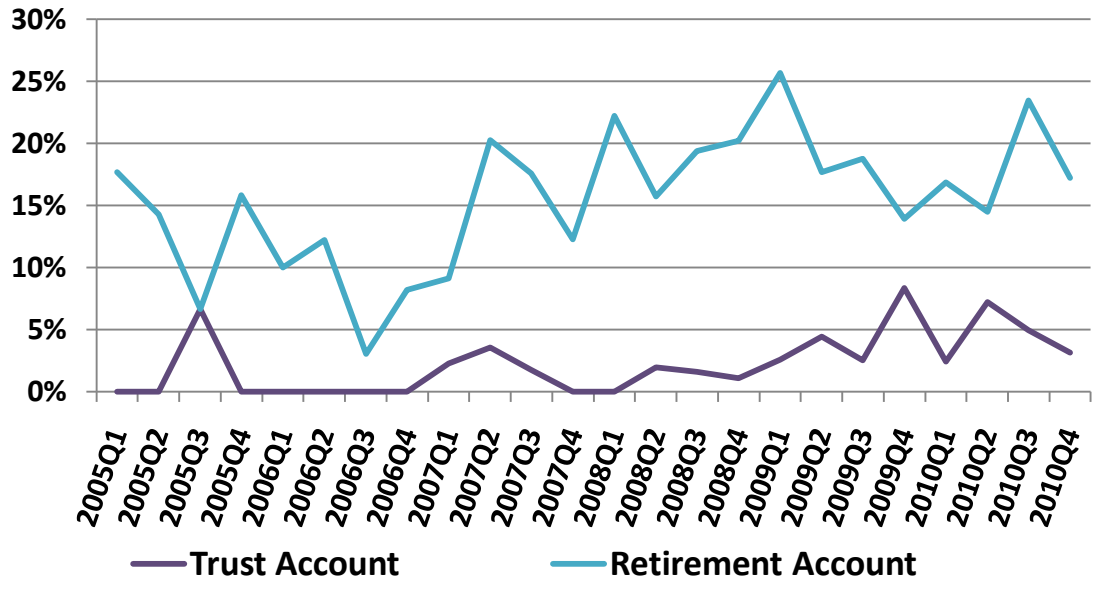
Graph 8 demonstrates that over the period of the first and second studies, identity thieves continued to favor the direct theft of funds from victim accounts. However, from the fourth quarter of 2006 through the second quarter of 2008, their focus shifted towards unauthorized trading in victim accounts. The level of thieves' market manipulation reached a point of parity with theft of funds at the very beginning of this period. During the next year, identity thieves appear to have shifted attention to mainly sales of established securities from victim investment accounts, causing the theft of funds line to trend up as well. Following the second quarter of 2008, the focus shifted decisively back towards the direct theft of funds. The drop in reported unauthorized securities transactions in victim accounts suggests that thieves favored victim accounts holding significant cash balances. This data appears to correlate with the upswing in retirement account abuse shown in Graph 9.

Specific Types of Investment Accounts

The majority of relevant sample filings reported the abuse of individual investment accounts. Financial institutions specified the abuse of retirement accounts in nearly 16.5 percent of filings and abuse of individual or family trust accounts in over 2.5 percent. The trend in abuse of both retirement and trust accounts was up strongly as noted in Graph 9.

GRAPH 9

Percentage of Quarterly Sample Filings Reporting Abuse of the Noted Investment Account Types



Holders of retirement accounts may either be incapacitated or, in some instances, deceased. Such circumstances might allow identity thieves, especially relatives or caregivers, the opportunity to abuse the accounts without immediate detection.[24] An analysis of elapsed times between last identified suspicious activity and detection indicates that average detection times associated with retirement account abuse are somewhat longer than for fraudulent activity targeting other account types. Additionally, many retirement accounts, especially those held by individuals who are already retired, are more likely to hold a higher percentage of assets in safer, more liquid, and easier to transfer holdings such as money market accounts, making them potentially more attractive to thieves.

Nearly 65 percent of the retirement account-related sample subset reported the takeover of an existing victim retirement account (trend modestly declining). Just under 9 percent of the subset reported the thieves' set up of an unauthorized retirement account using stolen identifiers with the apparent intent to defraud (trend was modestly down). About 30.5 percent described retirement accounts set up by employers on behalf of employees who apparently stole the SSNs of identity theft victims to secure employment, rather than to directly defraud the victims or the filer (trend was modestly down).[25]

More than 4 percent of the subset reported thieves' attempts to rollover funds from existing victim retirement accounts to new unauthorized retirement accounts, with all but one filing submitted in 2009-2010.

Just over 1 percent of filings reported the thief's unauthorized set up of accounts titled as corporate investment accounts. The thief used the identifying information of legitimate established companies and generally funded the account with one or more checks payable to the victimized company that the thief had stolen from the mail. These checks generally cleared the banking system without difficulty, allowing the thief to drain the account before the theft was discovered (the reporting trend was moderately down).

---

24. Relatives and other acquaintances were the identified or suspected identity thieves reported in more than 17.5 percent of the retirement account-related sample subset; a percentage proportionally more than three times that reported in the overall sample. The reporting trend was up sharply.

25. Some filers reported both account takeovers and unauthorized new account set ups on the same SAR-SF.

Depository Account Abuse

As expected in a sample of SAR-SF filings, investment accounts were the most frequently referenced account type. Nevertheless, depository accounts figured prominently in reporting as well. Overall, somewhat less than 25 percent of sample filings reported the abuse of one or more existing legitimate depository account(s) and/or the unauthorized set up of one or more new depository account(s) using stolen identifiers. The trend in reporting of depository account abuse was slightly up.

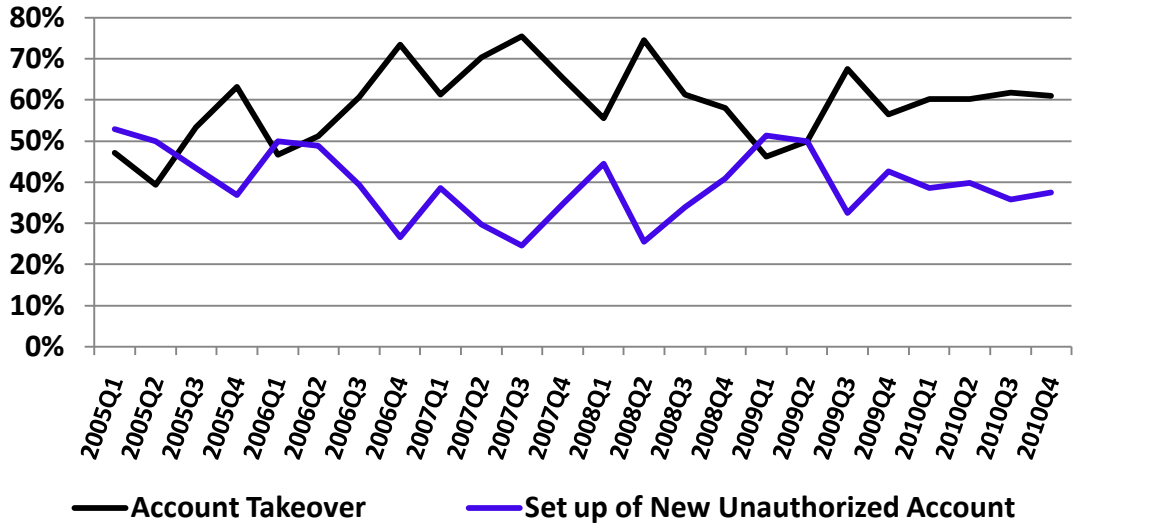
The great majority of affected depository accounts were individual accounts. Nonetheless, nearly 3 percent of the accounts were corporate accounts (the reporting trend was moderately up).

Account Status Preference

Graph 10 indicates the quarterly percentages of sample filings reporting the identity thief's abuse of one or more existing legitimate victim accounts versus the unauthorized set up of one or more new accounts using stolen identifying information.[26]

GRAPH 10

Percentage of Quarterly Sample Filings Exclusively Reporting Account Takeovers vs. Those Including Report of New Unauthorized Accounts Set Up



26. Many filings report the thief's abuse of more than one account. Some reports describe both legitimate existing and new unauthorized accounts or both investment and depository accounts. Graph 10 compares percentages of sample filings exclusively describing the abuse of existing legitimate victim accounts versus the percentages of sample filings including a report of the set up of one or more unauthorized accounts using stolen identifiers.

The identity thief's apparent preference during most quarters for taking over legitimate existing victim accounts versus setting up one or more new account(s) using victim identifiers likely correlates with the thief's relative success and ease in stealing funds. Analysis of sample narratives indicated that filers generally placed new accounts under closer scrutiny and often restricted the volume and value of activity that could occur in new accounts for some period of time.

Additionally, customers' ability to view their prior account activity online could allow the identity thief to both note typical customer activity on the account and possibly gauge the frequency of customer account monitoring. Consequently, an identity thief who is able to take over an established account may be able to closely mimic prior account activity while also draining funds from the account, thus escaping detection for some time. Account holders who view their account activity infrequently may put their accounts at greater risk.

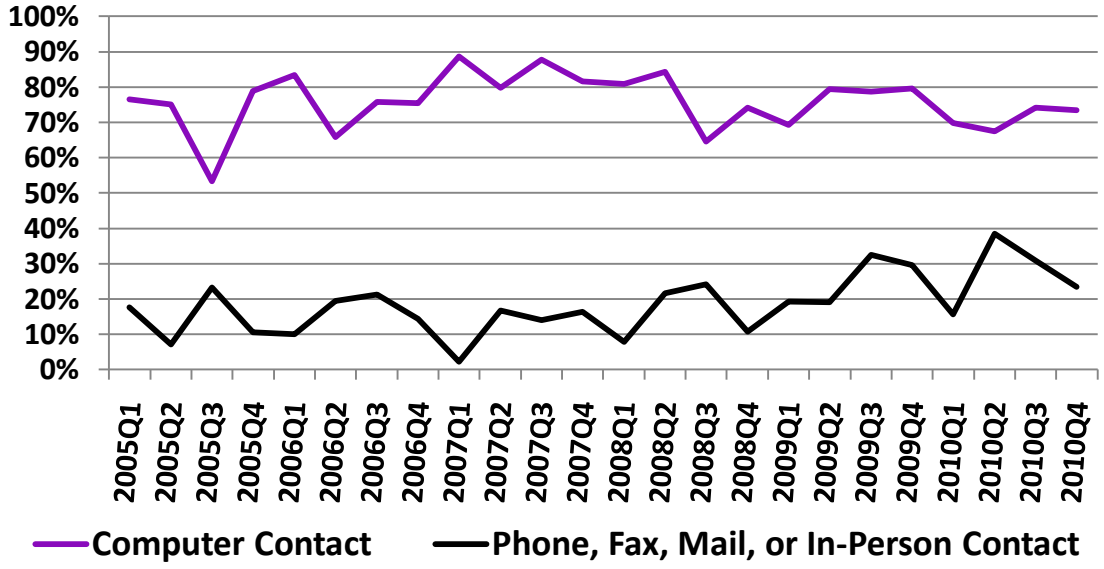
Identity Theft Facilitation

Means of Contact

The sample data highlight the great value of the computer to identity thieves, but also demonstrate the continued value of the phone, fax, and even the standard letter to facilitate both identity theft and the resulting financial fraud. Graph 11 displays the quarterly percentages of sample filings reporting the identity thief's reported means of contact with the filer.

GRAPH 11

Percentage of Sample Filings Clearly Reporting Manner of Identity Thief Contact with Filer



In many instances, the thief used both computer and non-computer communications to misrepresent his or her identity and steal funds.

Overall, nearly 19.5 percent of sample filings reported the thief's use of the phone to facilitate identity theft or commit financial fraud. Since the phone was the primary means of non-computer identity thief contact reported in the sample, the phone was mainly responsible for the ascending trend line seen in Graph 9. About 2 percent of filings after 2008 reported the use of Voice-over-Internet Protocol (VoIP) phone lines to advance these ends. Since VoIP numbers are trunk lines not attributable to any given computer device, it is likely the thief used them to avoid detection. Nearly another 1.5 percent of filings after 2008 reported the thief's use of phone relay services, generally intended for use by the deaf. Thieves may have used relay services to avoid providing the filer a voice print, as most filers retain voice recordings of customer calls.

Likewise, about 5.5 percent of filings described the thief's use of a facsimile machine, and somewhat more than 4 percent noted use of the U.S. mail or a private carrier for the same purposes. In a few instances (somewhat less than 1 percent of filings), the identity thief contacted the filer in person. Trends in reported fax and mail contact were slightly down, whereas personal contact, though still rare, was trending up.

Means of Computer Intrusion

Overall, 16.5 percent of sample filings reported the means by which the identity thief was able to gain access to the victim's computer. In somewhat more than 15 percent of filings, malware was found on the victim's computer. In almost 1.5 percent of filings, the victim admitted to being duped by a phishing email that led to a spoofed Web site. This group also included the more than one half percent of filings in which victims admitted accessing their financial accounts from public computers, including public computers located in third world countries. One filer reported that a contract employee admitted to accessing customer information from a public computer, resulting in the exposure of several thousand customer records. Identity thieves were shown to have hacked into personal or corporate computers in about one half percent of filings.

Unauthorized Alteration of Account Information

Identity thieves who gained access to a victim's existing account(s) often added or changed account information. The most significant changes included the linking of one or more accounts to an investment account. Overall, somewhat more than 8.5 percent of filings reported a thief's addition of one or more linked account(s) to the victim's investment account(s). The linked accounts, virtually always depository

accounts, were intended to receive funds drained from the investment accounts.[27] The trend noted for this facilitator was significantly up, with proportionally almost twice as many filings reporting this activity in the second study period as in the first. Much less frequently (about 1 percent of filings), thieves added a bill pay feature to the account(s) and used this feature to order payments either to themselves or to apparent creditors.

Some thieves reportedly changed other account information as well, apparently to temporarily delay the victim's discovery of thefts from accounts and/or to facilitate receipt of stolen funds. Thieves changed the victim's mailing address in almost 4.5 percent of filings, the email address in somewhat more than 3 percent, the phone number in about 3 percent, and the account password in close to 1.5 percent of filings.[28] In a few filings, thieves reportedly forwarded the victim's phone calls to phones they controlled during the period they actively stole funds from the victim account(s). Several recent filings reported a variation on this theme, with the thief inundating the victim's phone with spam calls while conducting fraudulent activities within the victim's account.

Relationships

Another significant facilitator concerned the thief's ties to the victim through family, friendship, employment, or business relationships. Overall, close to 5.5 percent of filings reported a relationship that likely provided the thief unfettered access to the victim's personal identifiers. The reporting trend for this facilitator was up moderately over the course of the two studies.

Internet Work Scams & Unwitting Participants

Though reported in relatively small numbers, sample filings did highlight a steeply increasing trend in reporting concerning individuals who are conned into becoming unwitting participants in identity theft and financial fraud through Internet work scams. About 1.5 percent of the overall sample reported this activity, but the relative incidence reported in 2009-2010 was three times that reported in 2005-2008. In general, these filings reported that the identity thief initiated the unauthorized

27. Several filings did report other investment accounts, online payment accounts, or prepaid card accounts as the linked accounts.

28. Thieves frequently made nearly imperceptible changes to victim email addresses such as adding or deleting one letter or punctuation mark, apparently in hopes that the filer would not notice the change. In some filings, thieves reportedly changed physical addresses by altering apartment numbers or by transposing street numbers with the same intent.

transfers of funds from victim accounts to the personal accounts of the thief's unwitting "employees." The duped individual then generally sent the money on to the thief minus an agreed "fee."

Different Victims, Same Thieves

Filers frequently reported more than one victim per filing. In many cases the filer did so because the identity thief used the same bank account number, phone number, IP address, media access control (MAC) address, physical address, and/or email address to facilitate theft from multiple victims. Overall, nearly 8 percent of filings reported a thief associated with the same IP address attacking the accounts of multiple victims. Several of the most recent filings reported the same MAC address used to defraud multiple victims, meaning that the same access device was used in multiple thefts.[29] Filers reported same bank account numbers in about 2.5 percent of filings, identical phone numbers in somewhat more than 2 percent, like physical addresses in just over 2 percent, same email addresses in somewhat more than 1 percent, and other types of links in something over 1 percent of filings. Given that many filers maintain recordings of customer phone calls, around one half percent of filings even linked the same individual to multiple victims through the alleged thief's voice print.

Identity Theft/Financial Fraud Rings

Overall, about 1.5 percent of filings attributed reported activities to groups of individuals conspiring in identity theft/financial fraud rings.

In an evaluation of the overall population of identity theft-characterized SAR-SF filings submitted between 2005 and 2010, FinCEN identified 109 filings out of 10,259 that included "ring" in the SAR-SF narrative in context. The majority of the earlier filings (77 submitted between 2005 and the third quarter of 2008) were recurring reports on the operations of the same rings. Prominent (35 filings) among these were reports describing the operations of a ring apparently based in Central Europe. This ring engaged in the direct theft of funds from investment and depository accounts and employed ACH to move stolen funds into corporate accounts it controlled. Much of this activity also appeared to involve unwitting "employees" of the ring members who responded to Internet work scam emails and provided their personal bank accounts as intermediary collection accounts for this activity.

---

29. A media access control address is a unique machine identifier hardwired into the network card contained within the computer or hand-held device. See http://www.techterms.com/definition/macaddress.

A group of 11 filings concerned a ring that conducted unauthorized trading in victimized investment accounts and then drained funds using ACH. Another group of 5 filings described the operations of a ring apparently based in West Africa.

Overall, at least 44 of 77 filings reported the operations of rings apparently based outside the United States, including 3 describing the operations of a ring likely based in South America. Of the remaining 33 filings, 7 specifically identified U.S. cities in which rings appeared to be based, while 5 described rings operating throughout the U.S. or within specific geographic regions.

Research located an additional 32 filings made between the fourth quarter of 2008 and the end of 2010. Of these, 8 filings described the operations of a ring draining funds from multiple depository accounts at the same institution, and transferring these funds to accounts at the same investment firm.

Another 5 filings described the operations of a ring that took advantage of an inadvertent online breach to steal money from corporate accounts. This particular breach occurred when bankruptcy filings posted online for a specific company accidentally included the corporate bank account numbers of all of the company's creditors.

Though just 1 filing among the 32 identified a ring apparently based outside the U.S. (in Asia), sample study data taken from the same period did describe the operations of a ring whose members were all apparently university students from the same Central European country.

Another 7 of the 32 filings described rings based in specific U.S. cities. A ring described in 1 filing garnered its illicit funds through student loan fraud, while another ring referenced in 1 filing profited from auto and mortgage loan fraud.

Customer and Employee Database Breaches

Though the number of total filings remained low, an increasing number of filings reported the financial results of identity theft facilitated through customer or employee database breaches. Overall, somewhat over one half percent of sample filings reported breaches in which personal identifying information on thousands of individuals was inadvertently or intentionally exposed to potential abuse.

Discovery

Identity theft was often uncovered through multiple, often complimentary, means. Filers most frequently discovered identity theft through their normal account monitoring procedures (about 53 percent of sample filings). In about 51.5 percent of filings, the person whose identity was stolen confirmed filer suspicions that he or she had suffered identity theft or notified the filer of the theft. Filers credited public database searches for revealing identity theft in about 9 percent of filings. Other reported means of discovery included questionable documents (nearly 2 percent of filings), and contact with the identified perpetrator (over 1.5 percent of filings). A law enforcement agency or a tax authority notified the filer of identity theft in close to 1.5 percent of filings each.

Mitigation

Filers and identity theft victims mitigated the effects of identity theft-facilitated financial fraud by rejecting proposed account applications or transactions, completely or partially stopping payment on transactions that had already been executed, and/or by contacting authorities and increasing account security measures after the attempted or successful financial fraud occurred. Table 8 lists the most frequently reported preemptive, proactive, and post-event mitigators employed by filers or victims.

TABLE 8

FILINGS REPORTING	*2005-2008*	*2009-2010*
Account Restricted	27.70%	30.62%
Transaction Successfully Recalled/Stopped After Execution	17.20%	24.39%
Transaction Rejected Prior to Execution	20.09%	17.21%
Account Closed	18.87%	13.41%
Computer Checked/Cleaned for Malware	9.44%	8.13%
Law Enforcement Contacted	8.37%	7.32%
Victim Affidavit of Forgery Completed	5.33%	5.33%

Recent sample filings reported that some filers issue random password generating tokens to their clients. The client logs on with the temporary password number generated by the token. Because the token issues a new temporary password number each minute, key logging malware or other similar viruses maliciously installed on a client's computer collect information that is almost immediately useless to the identity

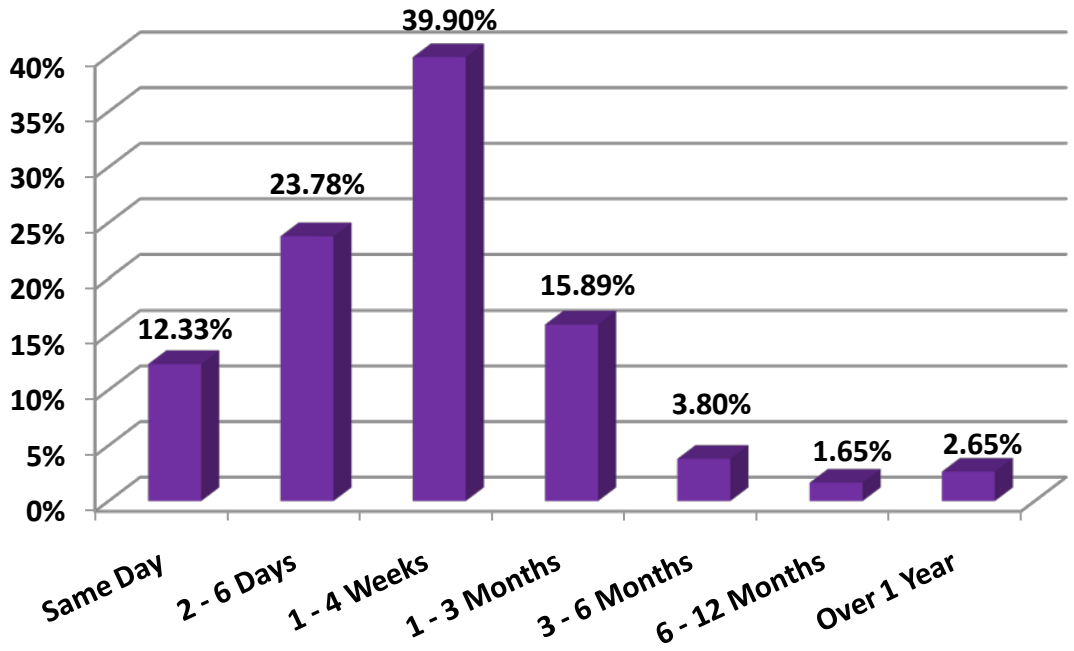
thief. Somewhat more than 2.5 percent of the second study filings referenced issuance of these tokens to customers. Nearly 1 percent of sample filings from 2009-2010 referenced the issuance of spoken passwords that customers would presumably not record on their computers.

Time Elapsed Between Last Identified Suspicious Activity and Discovery

Graph 12 displays the percentage of filings made during different time periods following the last identified suspicious activity.

GRAPH 12

Time Elapsed Between Last Identified Suspicious Activity and Discovery



As the graph shows, in about 76 percent of relevant sample reports, the filer discovered the suspicious activity within 4 weeks of the last identified suspicious activity.[30]

30. Estimates were made based upon reported dates of discovery and last identified activity rather than upon SAR-SF filing dates.

Identity Theft Red Flags

Though only one sample filing specifically referenced requirements under the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), most filings reported one or more activities consistent with at least one FACT Act Identity Theft Red Flag, or a derivative thereof.[31] About 76 percent of sample filings essentially reported "The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor."[32] The trend in reporting for this red flag was flat.

In over 38.5 percent of the sample the filer reported discovery consistent with "The financial institution or creditor is notified by a customer, victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft."[33] The reporting trend was mildly up.

Other frequently reported identity theft red flags in the sample were, "Shortly after the notice of a change of any covered account attribute, the institution or creditor receives a request for the addition of a linked financial account or automatic payment feature to a covered account" (9.5 percent of filings with trend strongly up);[34] "The Social Security Number provided is determined to belong to an individual other than the presenter" (8.5 percent of filings with trend mildly down);[35] "Shortly after the notice of a change of any covered account attribute, the institution or creditor receives a request for a change in one or more other account attributes including linked bank accounts, address, linked credit card accounts, email address, phone number, or account password" (close to 8.5 percent of filings with flat trend);[36] "The Internet protocol (IP) address or computer device number used to open a new account or access an existing account is the same as that associated with prior unauthorized account activity" (nearly 8 percent of filings with flat trend);[37] "A covered account

31. See 16 CFR 681.1. See also, *The SAR Activity Review – Trends, Tips & Issues*, pages 40-44 (October 2008), available at http://www.fincen.gov/news_room/rp/files/sar_tti_14.pdf.
32. Red flag 25 in Supplement A to Appendix A in 16 CFR Part 681.
33. Red flag 26 in Supplement A to Appendix A in 16 CFR Part 681.
34. Analysts derived this red flag during this study.
35. Analysts derived this red flag during this study.
36. Analysts derived this red flag during this study.
37. Analysts derived this red flag during this study.

is accessed from an IP address or device number not consistent with established patterns of access" (nearly 6 percent of filings with trend moderately up);[38] "The Social Security Number provided is determined to be unissued or assigned to an individual reported as deceased" (about 4 percent of filings with trend moderately up).[39]

Less frequently, filers described the following identity theft red flags: "The financial account linked to a new account application is the same as that associated with prior unauthorized account activity" (2.5 percent of filings with trend sharply up);[40] " For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report" (2.5 percent of filings with trend moderately up);[41] "The phone number linked to a new account application is the same as that associated with prior unauthorized account activity" (somewhat more than 2 percent of filings with trend sharply up);[42] "The address linked to a new account application is the same as that associated with prior unauthorized account activity" (a bit over 2 percent of filings with trend sharply up);[43] "The person opening a covered account or the customer fails to provide all required personal identifying information on the application or in response to notification that the application is incomplete" (just over 2 percent with trend sharply down);[44] "A fraud or active duty alert is included with a consumer report" (about 2 percent of filings with trend strongly up);[45] "Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account" (1.5 percent with trend moderately down);[46] "The email address linked to a new account application is the same as that associated with prior unauthorized account activity" (somewhat over 1 percent of filings with trend moderately up).[47]

Filers reported all other identity theft red flags in less than 1 percent of filings.

---

38. Analysts derived this red flag during this study.
39. Red flag 10b in Supplement A to Appendix A in 16 CFR Part 681.
40. Analysts derived this red flag during this study.
41. Red flag 18 in Supplement A to Appendix A in 16 CFR Part 681.
42. Red flag 12b in Supplement A to Appendix A in 16 CFR Part 681.
43. Red flag 12a in Supplement A to Appendix A in 16 CFR Part 681.
44. Red flag 16 in Supplement A to Appendix A in 16 CFR Part 681.
45. Red flag 1 in Supplement A to Appendix A in 16 CFR Part 681.
46. Red flag 23 in Supplement A to Appendix A in 16 CFR Part 681.
47. Analysts derived this red flag during this study.

Reported Cooperation between the Filer and Other Affected Financial Institutions

Filers reported their filing of a notice with FinCEN under section 314(B) of the USA PATRIOT Act in just under 1 percent of filings, with reporting trending up moderately. However, the level of unofficial cooperation described in sample filings between financial institutions affected by identity theft-facilitated financial fraud was significant, and was generally limited only by written filer policies intended to safeguard customer privacy. Analysis of sample filings indicated that filers who felt active contact with another financial institution was warranted (over 15 percent of filings) received sufficient information from the contacted financial institution to establish whether identity theft had occurred in nearly 96 percent of reported contacts. The level of effective cooperation reported remained steady from 2005 through 2010.[48]

Filings of Special Note

During this study, FinCEN noted many uncommon and novel schemes and tactics identity thieves employed to further their efforts. Filer reports of these activities, especially those that resulted in successful financial fraud, may point to future trends. The summaries below illustrate the variety of activities that filers reported.

Attempts to Keep Fraud Hidden

- A phone caller apparently used a voice altering device while employing social engineering tactics in attempts to gather customer account information from a filer employee (vishing).
- A filer's voice log tied the same caller to fraudulent activity conducted in numerous customer accounts.
- A fraud ring invested in securities using funds stolen from credit cards. The ring members invariably made profitable trades with the funds and immediately re-credited the credit cards from which they had stolen funds with the exact

48. Of the total 1,395 relevant sample filings encompassed in the earlier and later study data, 212 described active contact between the filer and one or more other affected financial institutions. Active contact was defined as any contact beyond the passive contact generally associated with rejected items processing.

amounts of the original charges, thus frequently hiding the original unauthorized charges. Ring members then sent the profits by ACH to business accounts located in the same states where the legitimate credit card holders resided.

- Another ring of identity thieves traded in foreign exchange markets and then moved profits to multiple personal accounts located throughout the United States.
- An identity thief took over multiple customer accounts. The thief apparently used account balances to manipulate share values in thinly-traded securities. The thief also purchased and sold shares of established securities the legitimate account holders had previously traded, thus apparently attempting to make transactions in the accounts appear legitimate.

Corporate Identity Theft

- A work-from-home scam operation based offshore used the name of a legitimate company in its contact with individuals. After interested persons completed an online questionnaire, they were tricked into collecting stolen funds for the operation.
- A fraud ring abused a bank's name to sell fraudulent certificates of deposit.

Insider Identity Thieves

- An employee of an insurance filer issued annuity contracts totaling several million dollars to individuals unrelated to the annuitants. Filer investigation determined that the named annuitants were under hospice care and that the employee had either forged their signatures on the annuities or tricked them into signing the annuity contracts without their informed consent by misrepresenting the purpose of the forms. The filer terminated the employee.[49]
- A former employee of an insurance firm stole hundreds of thousands of dollars from customer accounts, representing withdrawals as partial refunds of prepaid annual premiums or as partial surrenders of policy cash values. The thief persuaded a friend to launder the funds through the purchase of gift cards, claiming the funds came from the thief's gaming winnings that the thief was trying to hide from the spouse.

---

49. See similar activities described at http://dockets.justia.com/docket/rhode-island/ridce/1:2009cv00471/26958/.

- Several filings recounted the operations of investment con men. These individuals generally had prior legitimate positions with recognized investment companies and were thus able to persuade victims to allow them to invest their funds. Once these individuals had secured victim funds, they made highly speculative trades without their investors' consent and denied the investors control over their own funds.
- A filer's employee listed an account holder's identifiers on a loan application for the employee's relative, making the account holder a co-signer on the loan without the account holder's permission. Investigation indicated that the employee had likely defrauded other account holders.
- Relatives of a deceased former annuitant continued to collect annuity payments following the annuitant's death. The annuitant's insurance agent was complicit in the fraud.

Mail Theft

- An identity thief stole a client's tax return documents from the mail. The thief submitted the documents to the Internal Revenue Service (IRS) after substituting his own address as the return address, thus garnering a tax refund based upon investment losses claimed by the victim.
- A multi-million dollar identity theft/fraud ring stole bank statements from the mail stream in a Latin American country. The ring used the account information to drain money from depository accounts, which it then used to open investment accounts. Once funded, the ring liquidated the investment accounts and had the money sent to a mail drop. The mail was then forwarded to a foreign address.
- A filer received multiple unauthorized online change-of-address requests directing that addresses be changed from U.S. addresses to addresses in Russia and the Baltic states. The affected accounts belonged to nursing home residents.

Database Breaches

- An identity thief apparently hacked into a state's sex offender registry to retrieve the personal identifiers of the registrants. The thief then used the identifiers to set up unauthorized investment accounts. The filer discovered the scheme by searching victim names on the Internet.

- A filer's former employee sold several dozen sets of account holder identifiers to identity thieves.

Stolen or Forged Documents

- A mortgage company contacted a brokerage to verify customer investment balances. The brokerage determined that the mortgage applicant had obtained a customer's account statement and was representing himself as the customer in order to secure a mortgage based on the victimized customer's investment account balance, and presumably also intending to secure the mortgage in the customer's name.
- An identity thief apparently impersonated an account holder and used one of the account holder's statements to secure financing to purchase a large life insurance policy.
- A ring used fake IRS notification letters and forms to gather sensitive identifiers from non-resident aliens. The thieves used bank information provided to clone victim debit cards and drain depository accounts.
- A company insider forged the signatures of company officers authorized to disburse large amounts of company funds. The forgery resulted in an unauthorized filer transfer of hundreds of thousands of dollars to an individual known to be involved in financial fraud located in a third-world country.
- A law enforcement investigation turned up a power of attorney and a fake death certificate associated with an identity theft victim. Investigators determined that a corrupt notary created the documents.
- An applicant for a new account submitted a phony driver's license photograph copied from an official publication on identity document evaluation.

Computer Intrusion

- An account holder travelled throughout the country installing key logger viruses on public computers available to guests in high-end hotels to gather bank and investment account information, which he used to drain their accounts. The filer submitted a SAR to report that the account holder was arrested for a multi-million dollar identity theft financial fraud spree.

- An identity thief hacked into a customer's email account. The thief then posed as a person to whom the victim was contracting work in the victim's home, and had the down payment for the work re-directed to the identity thief.

Prepaid Cards

- An identity thief opened new investment accounts funded with unauthorized ACH debits he initiated against depository accounts. As soon as the money was transferred to the investment accounts, the thief transferred it to other apparent depository accounts, later determined to actually correspond to prepaid card numbers.
- An identity thief submitted a loan application against a client's account. The account number on the voided check attached to the application to allow the filer to set up an ACH transfer to the purported checking account of its customer proved to be a prepaid card number instead. The check was counterfeit.

Tax Evasion & Money Laundering

- Relatives of a deceased individual set up an account in the deceased's name years after his death to deposit stock certificates payable to the deceased. Motives may have included tax evasion and/or attempts to avoid probate of the assets.
- A filer identified a sophisticated tax evasion scheme engineered by a wealthy, highly-experienced investor. The investor invited college students to open investment accounts, which the wealthy investor funded completely with his funds. After one year, the investor split any profits made in the account with the student. All profits were recorded against the student's identifiers as the account holder. At the end of the year, the investor led the college student to believe that the account was closed. In many instances, the investor left the accounts open and continued to use the accounts for investments. Since the accounts were titled to the students, trading profits were recorded against the student's identifiers, but taken by the investor. Though not reported, it is presumed that the investor did eventually close the accounts before the students graduated and began making significant amounts of reportable income.
- An identity thief used stolen identifiers to open both investment and depository accounts. The fraudster used these accounts over a multi-year period, making large trades in thinly-traded securities. The filer found no indication that the funds were stolen, raising the possibility that the fraudster used the accounts to launder funds and/or evade taxes on trading gains.

- An individual opened an investment account in his mother's name. The filer determined that the individual had sizable state and federal tax liens, suggesting he used his mother's identifiers to evade taxes or payment of the liens from any profits arising from account transactions.
- Several individuals deposited counterfeit physical share certificates of a legitimate company to multiple filer accounts. Subsequently, other individuals bought these counterfeit shares. The described activity appears to indicate that the corporate identity thieves used filer accounts to launder significant amounts of money by making the movement of funds from one investor to another appear to be legitimate investment activity.

Market Manipulation

- A company located in a Baltic country apparently took over client investment accounts and used account balances to manipulate the market in certain thinly-traded securities.
- A clearing broker reported that multiple firms that clear their trades through the filer reported that identity thieves compromised credentials belonging to their brokerage employees. In each reported instance, the identity thieves used the credentials to purchase the same thinly-traded security, presumably to drive up the share price to make their sales of the same security held in other accounts profitable.
- An individual opened unauthorized investment accounts using stolen identifiers. The fraudster then used the accounts to manipulate share values of thinly-traded securities, reaping half a million dollars in illicit profits.

Abuse of Promotional Account Features

- A few filings recounted use of stolen identifiers to set up unauthorized accounts and then take advantage of a filer's promotional account features. After setting up each account, the thief used the supplied ATM card to make hundreds of small withdrawals of about $10 each. One of the filer's selling points was that it refunds all customer ATM fees on accounts. The thief made all of the withdrawals from the same independently-owned ATM, one that charged a $20 fee for each transaction. The filer lost thousands of dollars refunding the thief's ATM fees. The filer did not indicate whether the thief either owned the ATM or had struck a deal with the owner of the machine to share the exorbitant fees charged.

- Another identity thief set up hundreds of unauthorized accounts using stolen identifiers to take advantage of a promotional cash credit the filer offered on new accounts.

Other

- An identity thief used account holder identifiers to obtain prescription drugs.
- A probable con man claiming to be a member of a family known to have a multi-billion dollar fortune came to the filer with a potential business proposition. The individual directed the filer employee to a Web site that the individual purported would establish his claims. The filer employee noted that other than the recently-created Web site, he could find no information referencing the alleged billionaire.
- Several filings noted similar scenarios in which the filer received telephonic or fax requests, ostensibly from account holders living in a particular Latin American country. The requests directed that the filer debit funds from account holder investment accounts and wire transfer the funds to accounts at depository institutions in Latin America. Filers reported that they verified the received instructions through direct phone contact with the account holder at the phone number received in the original account application. Nonetheless, the account holder contacted the filer a week or two later claiming the withdrawals were unauthorized, raising the possibility that a ring whose members feigned victimization from identity thieves was operating to defraud filers.

BEST PRACTICES

A large number of filer practices noted in the study sample may ameliorate both the effectiveness and the effects of identity theft.

Filer Treatment of New Accounts

Based on analysis of the sample filings, it appears that most filers conduct public database checks of the information provided on new account applications prior to allowing an applicant to begin using the account. If the applicant's identifying information, such as Social Security Number, address, or date of birth, does not match public database information, the filer usually sends the application to its security office for further review.

After approving an application, many filers note the funding method employed by the new account holder. Generally, the filer will immediately restrict any new account if the initial funding instrument is rejected or returned by the paying institution.

Ongoing Filer Assurance of Customer Account Security

Many filings in the sample described measures filers employ on an ongoing basis to help ensure that their customer accounts are protected from unauthorized access, manipulation, or theft. Since a large percentage of all customer transactions now occur online, filers have devised means of verifying that the legitimate account holder initiated requested transactions. Online account access requires electronic passwords as a matter of course. Since passwords can be stolen through computer intrusion, many filers have resorted to issuing random temporary password generating tokens to their customers. As previously mentioned, these tokens generate new temporary account passwords that are only usable for a very short period, generally 60 seconds. Consequently, any key logging software surreptitiously installed on customer computers is of virtually no use to the identity thief since captured passwords are invalid by the time the thief receives them. It should be noted that this technology is not invincible to hackers.[50]

50. See http://gadgetwise.blogs.nytimes.com/2011/03/18/rsas-secure-ids-hacked-what-to-do/.

Another potentially valuable security measure is the employment of challenge questions. Overall, 2.5 percent of sample filings reported that a filer rejected requested transactions after receiving unsatisfactory responses to challenge questions. Though it is possible for legitimate customers to forget the answers to some challenge questions, the failure by the alleged customer described in one sample filing to remember the day or even the month of his wife's birthday could indicate identity theft.

Filers have also begun employing spoken passwords for account access. The customer calls the filer and provides this password to complete a transaction or receive account information. Since the password is not recorded on the customer's computer, it is not available to be hacked.

Many filers routinely telephone customers who request transactions online, by fax, or by letter whenever the request exceeds a dollar amount threshold. Filer employees are generally directed to contact the customer at the phone number provided at account opening to ensure that the employee is not calling a number recently added to an account by an imposter.

Many filers also insist that customers who have been victims of identity theft associated with computer intrusion have their computers professionally cleaned of any malicious software before allowing the customers to resume online access to investment accounts.

Filers also frequently verify with the paying institution that large ACH or negotiable instrument deposits to customer accounts are actually authorized by the account holder at the paying institution and that the paying account has sufficient funds to cover the transfer.

Addressing Specific Risks

Study findings noted the steeply increasing trends related to both the abuse of debit cards tied to investment accounts and the associated losses resulting from this abuse. Much of this activity is not initiated by the actual account holder, but involves debit cards stolen or cloned from legitimate customers. Possible mitigators include restrictions on debit card use by new customers and automated monitoring systems that temporarily restrict accounts exceeding set parameters to allow time for manual review of suspect transactions.

The study also noted the abuse of promotional account features, such as reimbursement for ATM charges. These abuses appear most likely when clear limits are not set on volume of transactions, aggregate dollar amounts, and/or maximum amount of ATM fee.

NEXT STEPS

Identity theft continues to plague the nation's consumers. The Identity Theft Resource Center (ITRC) recorded 662 data breaches in the United States in 2010, a nearly 33 percent increase from 2009.[51] The ITRC also reported in a June 2010 study that 87 percent of survey respondents were at least somewhat concerned about the threat of identity theft as they conducted online financial transactions.[52]

FinCEN will continue to monitor BSA filings related to identity theft and expects to issue additional reports on SAR reporting of identity theft within specific financial sectors.

51. See http://www.idtheftcenter.org/ITRC%20Breach%20Report%202010.pdf. Reference in this report to any specific commercial product, service, process, or enterprise, or the use of any commercial product or enterprise, trade, firm, or corporation name is for the information and convenience of the public, and does not constitute endorsement or recommendation by the Financial Crimes Enforcement Network. With respect to materials generated by entities outside of the Financial Crimes Enforcement Network, permission to use these materials, if necessary, must be obtained from the original source. The Financial Crimes Enforcement Network assumes no responsibility for the content or operation of other Web sites.
52. See http://www.idtheftcenter.org/artman2/publish/m_press/2010_Consumer_Survey.shtml.

www.FinCEN.gov