INSIDER FRAUD IN FINANCIAL SERVICES

CERT

Software Engineering Institute

Carnegie Mellon

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Insider Fraud in Financial Services

Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector

Insiders pose a substantial threat to financial services companies by virtue of their knowledge of and access to proprietary systems and their ability to bypass security measures through legitimate means.

Insider fraud is perpetrated by a malicious insider, which is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

WHAT YOU SHOULD KNOW

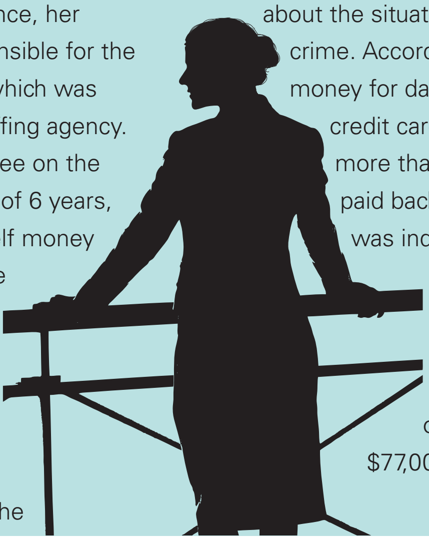
A recent study of insider fraud funded by the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and conducted by the CERT® Insider Threat Center, the U.S. Secret Service (USSS), the U.S. Department of the Treasury, and the U.S. financial services sector analyzed insider and outsider computer criminal activity in the financial services sector to help security professionals prevent, detect, and manage malicious insider activity and risk.

This document was derived from the research study's full report. The full report contains more information, including more detailed recommendations, fraud models that describe internal fraud activities, and more details about how the study was conducted.

The purpose of the research, of which this study is a part, is to identify indicators that predict insider fraud in the financial services industry and to formulate strategies to prevent or minimize damages from it. This particular study extracted technical and behavioral patterns from 80 fraud cases—67 insider and 13 external—that occurred between 2005 and the present. These cases were used to develop insights and risk indicators to help private industry, government, and law enforcement more effectively prevent, deter, detect, investigate, and manage malicious insider activity within the banking and finance sector.

A complete copy of the insider threat study, *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector,* is available at www.cert.org/insider_threat/. If you have questions that are not answered in this report, contact the Insider Threat Center at insider-threat-feedback@cert.org.

Paying a Fictitious Employee



Karen[1] worked as an accountant for a certified public accounting firm. Due to her good performance, her employer decided to make her solely responsible for the accounts of two client companies, one of which was her supervisor Alice's other business, a staffing agency. Karen eventually created a fictitious employee on the payroll of Alice's business. Over the course of 6 years, she used this fictitious identity to pay herself money from the staffing agency. Several times, she also issued fraudulent checks on behalf of the business and had them deposited to her personal accounts.

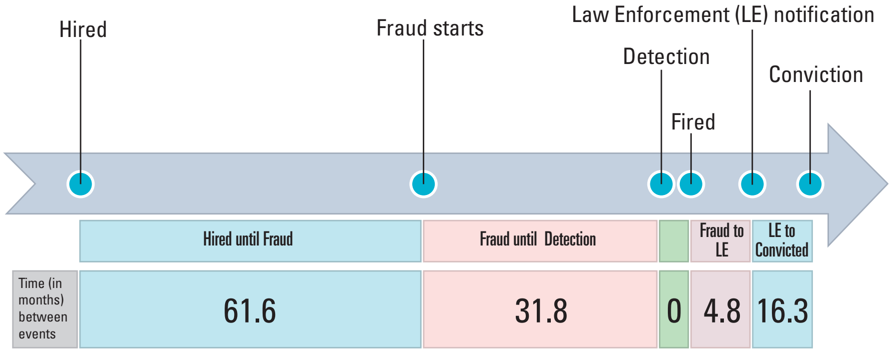
Karen was finally caught when Alice was preparing to buy a house and discovered a large amount of cash missing from one of the staffing agency's accounts. Alice confronted Karen about the situation, and Karen admitted to the crime. According to Karen, she stole the money for daily expenses and to pay her credit card debt. While she had stolen more than $100,000, she had already paid back approximately $23,000. Karen was indicted on charges of wire fraud and check fraud, and eventually pled guilty. She was sentenced to 15 months in prison and 3 years' probation and was ordered to repay the remaining $77,000 of the stolen money.

[1] Names used in this and other sample cases were changed to prevent the information being traced back to the company involved.

® CERT is a registered trademark owned by Carnegie Mellon University.

“Low and Slow” Approach

The study found that insiders who executed a “low and slow” approach to fraud accomplished more damage and escaped detection longer. In other words, the insiders stole “low” amounts of money and conducted their activities “slowly” over a long period of time, possibly to avoid detection.



Windows of opportunity exist during which fraud can be prevented or disrupted.

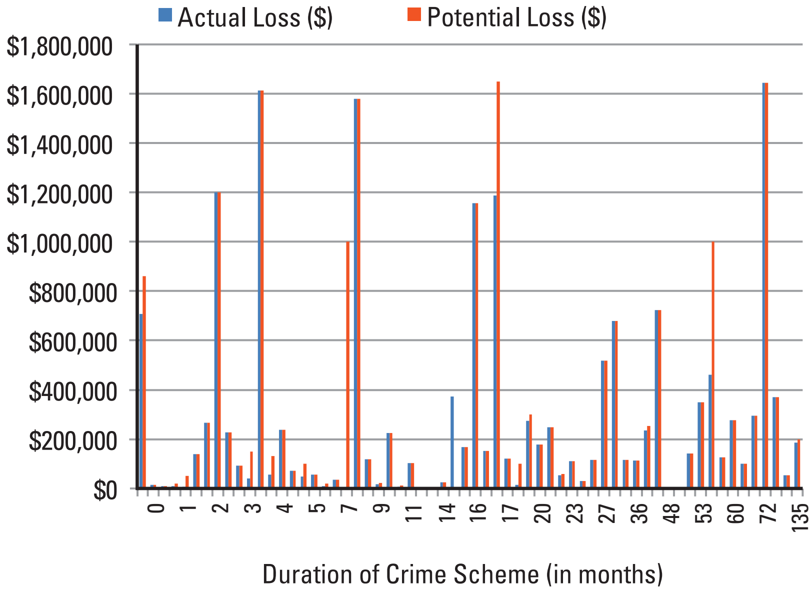
The “low and slow” crimes analyzed in this study had, on average, 132 fraud events over the course of the crime. The highest number of fraud events during a crime was 756 over a period of 47 months. The average number of thefts for a case 32 months or longer was 58 theft events.

On average, over 60 months (5 years) elapsed between an insider’s hiring and the start of the fraud.[2] An average of 32 months elapsed between the beginning of the fraud and its detection by the organization or law enforcement.

The good news about this “low and slow” approach is that the lengthy period of the fraud provides multiple opportunities to counter the fraud, if not prevent it.

The lower 50% of cases (under 32 months in length) had an average actual monetary impact of approximately $382,750, while the upper 50% (at or over 32 months in length) had an average actual monetary impact of approximately $479,000.

The study found that organizations were apparently effective at detecting the crimes that took place for short periods of time, even though the subjects were still able to cause significant financial damage. Organizations were not as effective at detecting the longer term crimes. The incremental damage (i.e., monthly, weekly amount stolen) was much lower in these cases, which may not have drawn as much attention. An average of nearly five months elapsed between when the fraud was discovered and the involvement of law enforcement.

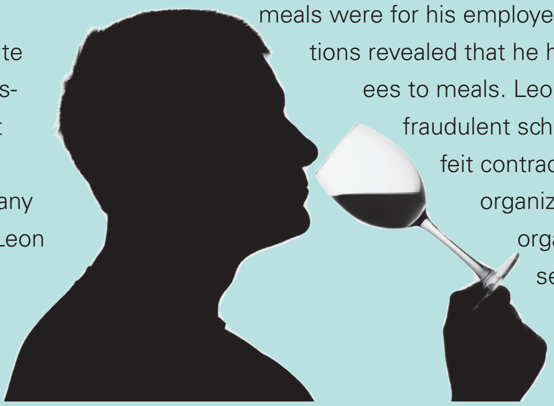


Longer duration crimes caused more financial impact.

[2] Though they often experienced personal or financial struggles that led them to commit fraud, there was not a known, common event (e.g., divorce, personal bankruptcy, change of work assignment) that immediately preceded or triggered the fraud.

Misusing the Corporate Credit Card

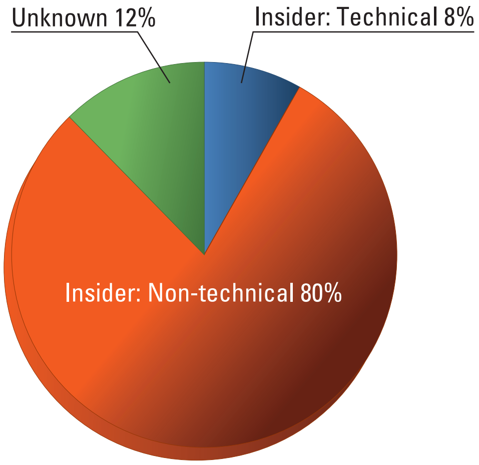
Leon worked as a vice president for a federal credit union. As part of his job, he was given a corporate credit card to use for business purposes only. Soon after being hired and continuing throughout his employment, Leon used this corporate credit card to pay for personal expenses. He also used the card to take out cash advances on a few occasions, even though doing so violated company policy. To justify the cash advances, Leon forged invoices on his business laptop and forwarded them to the appropriate departments within the organization. He also falsely claimed that the personal expenses on the card were for legitimate business purposes. For example, Leon used the card to pay restaurant bills and later claimed that the meals were for his employees; however, later investigations revealed that he had not treated any employees to meals. Leon was able to continue his fraudulent scheme by creating a counterfeit contract with his wife's third-party organization and then paying the organization for non-existent services via wire transfer.



"Low Tech" Tactics

The study found that most insiders' means were not technically sophisticated. In the cases analyzed, most insiders did not require technical knowledge (i.e., involving information technology, especially networks and computer systems) to commit the crime. They easily bypassed security controls or concealed their actions and exploited their organization's insufficient access controls.

The employees without technical knowledge or privileged access used systems to cause significant damage. Most insiders who used information systems to commit fraud used them for their intended purpose. For example, many insiders executed fraudulent wire transfers using information systems. Using the system did not require technical sophistication or extensive knowledge of the control mechanisms. It was merely the system that everyone used to complete that particular transaction.



Most insiders did not require technical knowledge to commit the crime.

Non-technical employees are most likely to commit fraud in the banking and finance industry. For example, if bogus vendors are added to a payroll system, the fraud is far less likely to be committed by a database administrator hacking into the payroll system than a payroll administrator who is responsible for paying vendors and has legitimate access to the system.

In the study, 71 percent of insiders who committed fraud relied on some form of authorized use or non-technical bypass of authorized processes. Of the 57 cases, 52 involved insiders using some form of previously authorized access to carry out the fraud. Non-technical subjects were responsible for 81 percent of incidents. Seven of those subjects were external attackers, but their methods were still non-technical.

In the few technical cases, the inherently greater level of privilege granted to technical insiders enabled their crimes. These privileges were often necessary for the insiders to perform their legitimate job duties.

Perpetrators' Position in the Company

Previous research into fraud activities indicates that non-managers were the primary perpetrators of malicious activity. In this study, which focused on the financial services sector, the research team found that two main types of insiders committed fraud:

- those who occupied senior positions (e.g., executives, branch managers)
- those who were more junior in the organizational structure

Of the insiders committing fraud whose role was known (e.g., teller, teller manager, vice-president), 51 percent were managers, vice presidents, supervisors, or bank officers. The remaining 49 percent did not hold supervisory positions, though they often served in fiduciary roles and may have had sufficient tenure at the organization to be very trusted.

Since more than half of these insiders were serving in supervisory roles, it is worth examining the differences between fraud committed by managers versus non-managers, such as differences in monetary impact and how they executed their crimes. The crimes of these two types of insiders show substantial differences.

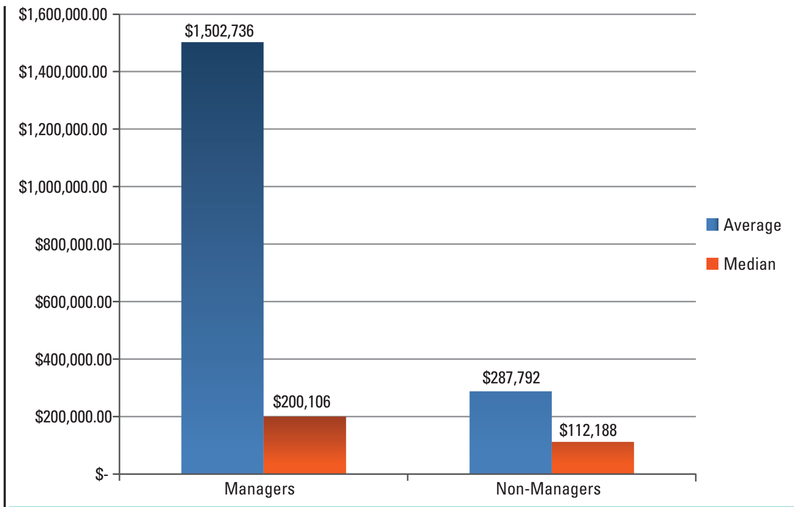
Cashing in Fraudulent Reward Points

Carl was a lead software developer at a prominent credit card company, which offered a rewards program where customers could earn points based on the volume and frequency of their credit card usage. These points could later be redeemed for gift cards, services, and other items of monetary value. Due to the high transaction volume of corporate accounts, a typical corporate account could hypothetically accumulate an immense number of rewards points. Therefore, the rewards points program was configured in such a way that the back-end software would not allow corporate accounts to earn points.

At an unknown date, Carl devised a scheme by which he could earn fraudulent rewards points by bypassing the back-end checks in the software and linking his personal accounts to corporate business credit card accounts of third-party companies. After compromising a co-worker's domain account by guessing the password, he successfully linked his personal accounts to several corporate accounts. Carl cashed in the rewards points for items of value, such as gift cards to popular chain stores, and sold them in online auctions for cash.

In all, Carl was able to accumulate approximately 46 million rewards points, $300,000 of which he was able to convert into cash before being caught by internal fraud investigators. Carl admitted to the scheme and bargained with investigators for a reduced sentence if he agreed to offer insight as to how organizations might prevent a similar occurrence from happening in the future.

The average monetary damage by managers seems very high, but it is skewed by one large outlier. The median values, which address outliers both high and low, may give a better sense of these numbers. The median results show that managers consistently cause more actual damage ($200,106) than non-managers ($112,188).



Managers exploited their superior access and lack of supervision to sustain longer crimes.

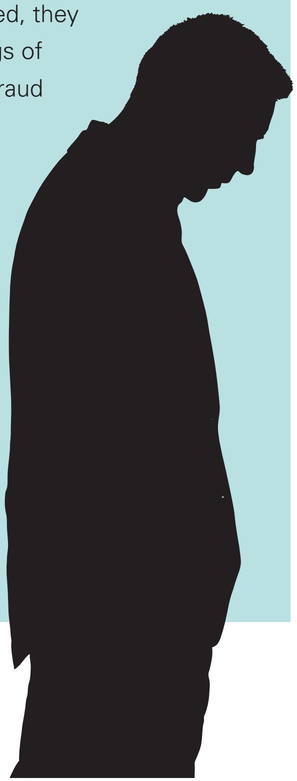
The study found that fraud by managers differed substantially from other employees by both damage and duration. Though their activities and access may have differed at times, managers and accountants caused the most damage from insider fraud. They also evaded detection for the longest amount of time. Many organizations in this study tended to blindly trust lead accountants or branch managers to do things for the right reason, even if their actions violated policies and procedures.

Supplying Information for Identity Theft

Ray worked as a branch manager of a national banking institution. Ray's father had a criminal history and while in prison had met a man who, after he was released, eventually started running an identity theft scheme. Sometime after being released, the father put his prison friend (Lloyd) in touch with Ray in the hopes that Ray would help steal account information using his privileged access. Lloyd offered to pay the insider $1,000 for each account.

While Ray initially refused, his father was eventually able to persuade him to take part in the fraud scheme. Over a three-month period, Lloyd asked Ray for the account information of 25 specific people. Ray divulged this information over the phone at work and on paper documents outside of work. Lloyd forged identifications using the account information and had a team of complicit cashiers who walked into banks and made fraudulent withdrawals.

In total, $228,000 was stolen. Once investigators received reports from customers whose accounts had been compromised, they were able to use the access logs of customer records to trace the fraud to Ray. He admitted to the scheme, and even helped investigators conduct a sting operation to apprehend Lloyd. Considering that Ray helped to catch Lloyd, who had an extensive criminal history and numerous charges, Ray was sentenced to time served and two years of supervised release.



Embezzling Loan Dollars

Carol worked as the loan processor for a banking institution. As part of her job responsibilities, she had full privileges to read and modify loan information within the organization. She took out two legitimate loans totaling $39,000 from her employer organization for her own personal expenses, which in itself was not a violation of company policy. However, to help pay for additional personal expenses, she used her privileged access several times to fraudulently increase her personal loan amounts. She then withdrew the resulting difference, thereby committing embezzlement. Carol was discovered when a routine audit revealed that essential loan documentation was missing from her loan account, which she had removed to cover up the fraud. By the end of her scheme, she had stolen approximately $112,000. Carol was sentenced to 18 months in prison and 5 years' probation and was ordered to pay full restitution.

Non-managers may be reluctant to report their supervisors when they violate rules, especially rules that seem to have little association with malicious or criminal conduct. For example, a manager, against the rules, insisted that he personally deliver customer account statements by hand in the name of good customer service. The manager did this because he had altered the statements and thought this exception would help him to avoid detection.

For fraud and other insider crimes, a factor was often the accumulation of access privileges over years of employment without reviewing the need for that access until it was too late. For example, if tellers or teller managers can complete account transfers, is it necessary that the branch manager also needs to be able to perform the same activity?

Crime duration also shows an interesting difference. Non-managers' crimes lasted an average of 18 months, while managers' crimes almost doubled to an average of 33 months. One explanation of this disparity in crime duration is that managers exploited their superior access to information and relative lack of supervision to sustain longer crimes.

Non-managers can be grouped into the following employment types:

- accounting (6 subjects)—employee whose primary responsibility is that of an accountant or equivalent
- customer service (14 subjects)—employee whose primary responsibilities are interacting with the organization's customers
- analyst (3 subjects)—employee whose duties dealt with some sort of analysis other than accounting activities
- technical (4 subjects)—employee whose duties dealt with some technical facet of operations, such as engineers or other IT personnel
- other (3 subjects)—anything that could not be accurately categorized as one of the above[3]

Table 1 shows the crime duration (in months), average actual damage (in dollars), and damage per month (in dollars) for the first four categories of non-managers.

[3] The "other" category is not included in Table 1 because the associated job roles were too disparate to be considered a coherent group.

Printing and Passing Account Information

Regina, a financial institution employee, accessed and printed account information belonging to multiple individuals. This information was then provided to Jeff, her boyfriend. Jeff then provided the information to his associates in New York who then recruited homeless or indigent people to enter financial branches, pose as legitimate account holders, and withdraw funds from the financial institution. The financial institution began investigating the missing funds and interviewed Regina, who confessed that she had printed the account information and passed it to an outside source. Regina was sentenced to probation (2 years) with home detention (6 months), random drug testing, and 50 hours of community service. She was also ordered to repay part of the stolen funds. The total losses exceeded $235,000.

Table 1: Comparison of Damage and Crime Duration by Non-Managers

	Accounting	Customer Service	Technical	Analysis
Duration Average, in Months	41	10	26	20
Average Damages, Actual	$ 472,096	$ 191,338	$ 104,430	$ 54,785
Damage per Month, Average	$ 11,627	$ 18,350	$ 4,041	$ 2,785

On average, accounting employees did the most actual damage followed by customer service employees and, with much less damage, technical and analysis employees. These numbers make sense because the accounting employees had the ability to illegally transfer funds and often had access to personally identifiable information. They were able to continue their schemes for the longest amount of time since they were often the first and last line of defense for proper accounting procedures.

Though customer service representatives were also able to cause significant damage on average, their schemes did not go on nearly as long; in fact, their schemes had the shortest duration of all. This short duration may have been because their activities were more easily audited and detected, and perhaps because they were generally not in supervisory roles and were thus unable to hide or explain their actions as justified exceptions to company rules.

Perpetrator Collusion

The study found that most cases do not involve collusion. Almost all cases that did involve collusion were perpetrated by non-managers; in fact, there was only one case of collusion that involved someone in a supervisory or management position. In addition, the cases that did involve collusion generally involved external collusion (i.e., a bank insider colluding with an external party to facilitate the crime). External collusions often involved an insider who wanted or needed an external party to act as a conduit to sell stolen personally identifiable information or pose as a legitimate account holder.

In this study, managers involved non-managers in their crimes largely without the non-managers' knowledge that the actions were criminal. The lack of internal collusion departs from previous research and findings about fraud collusion in general. For example, in previous research several instances of rings of insiders completing malicious activities together were captured—one such collusion was a ring of insiders at a government agency who issued fraudulent identification cards.

The vast majority of cases that involve collusion also involve the improper use of customer information or personally identifiable information. Clearly, the black-market value of such information motivates employees to undertake risky and illegal activities.

Some insiders who colluded with others used particularly low-tech means of exporting the information to their partners, such as reciting information over the phone or writing it on paper. In these cases, it seems there is virtually no technical detection measure that could be used to detect that data was being stolen. The insider's use of customer account information was caught after non-automated forensic audits revealed accounts with unusual activity.

Another group of cases involved the use of technology, but not necessarily in a particularly inventive or unique way. For example, one subject copied computer screens that displayed customer information; another copied and pasted personally identifiable information into text files; many more printed the information.

This study identified three types of collusion:

- *inside*—An insider recruited or was recruited by other employees.
- *outside*—An insider recruited or was recruited by parties completely external to the organization.
- *both*—The crime involved inside and outside parties. Either party could have done the recruitment.

For all insider cases, only 13 (16 percent) involved any type of collusion. This relatively small number departs from previous findings, both in other specific sectors and across all sectors.

Since the majority of fraud collusion in the financial services sector involved outside actors, it also seems that insiders often required external assistance to complete their crimes. For example, two cases involved inside employees paying outside entities (one of which posed as a vendor), who promptly withdrew money and shared it with the insider.

Seven other cases that involved external collusion dealt with the sale of personally identifiable information. In sectors other than financial services, internal collusion often occurs when it facilitates the crime or makes it more profitable. This advantage explains the single financial services case that involved internal collusion. The two insiders had separate access to personally identifiable information, and their collaboration facilitated the crime.

Fraud Detection

The study found that most incidents were detected through an audit, customer complaints, or co-worker suspicions. The large majority of cases were detected using non-technical methods. The organizations involved in the 80 cases were much more successful at detecting fraud by conducting audits, monitoring suspicious behaviors, and questioning abnormal activities.

The case data seem to indicate that technology played a very small role in enabling organizations to detect fraud. However, by itself, this finding could be explained or skewed by other factors. Perhaps technology was largely successful at preventing or detecting fraud before any damage occurred, thereby preventing incidents or stopping their further progression before law enforcement became involved.

Or, even if security systems collected information to detect fraud, the tools necessary to correlate the data may have been absent. Furthermore, the organization's IT staff may have been too busy with other tasks to adequately monitor the logs.

Data about the organization's detection and response to fraud proved scarce. Of the 80 cases in the study, just under half (45 percent) lacked information on how the incident was detected and by whom. Just over half (51 percent) lacked information about the type of logs used to detect and respond to the fraud. A fifth of the cases did not identify the primary actors who responded to the fraud.

In spite of the limited data available, the following conclusions can be inferred:

- The most common way that attacks were detected was through routine or impromptu audits. An audit detected insider fraud in 41 percent of the cases where detection methods were known. Other non-technical methods, such as customer complaints and co-workers noticing suspicious behaviors, were used to detect 39 percent of insider fraud. Only 6 percent of the cases involved fraud-monitoring software and systems, while the remaining cases used unknown detection methods.
- Over half of the insiders were detected by other employees, though none of the employees were members of the IT staff. This fact, combined with the mere 6 percent of cases in which software and systems were used in detection, seems to indicate that fraud-detection technology was either ineffective or absent. Most of the remaining cases were detected by customers, an unfortunate yet likely source of detection in cases of bank fraud.
- The case data contained limited information regarding the logs that were used during the detection and response phases. However, of the 62 cases with sufficient information, transaction logs, database logs, and access logs were used in 20 percent of the cases. About 10 percent of the cases showed strong evidence that no logs were used during detection, often because the insider readily admitted to the crime before the evidence was analyzed. The remaining 70 percent of cases presented evidence of log usage without specifying the type or exhibited a mixture of evidence, such as surveillance footage, phone records, print server logs, and system file logs.
- As expected, most initial responders to the incidents were managers or internal investigators (75 percent). Some cases (13 percent) also involved state or local law enforcement officials in addition to the Secret Service.

Personally Identifiable Information

The study found that personally identifiable information (PII) is a prominent target of those committing fraud. While we specifically excluded from the study cases involving simple cash drawer theft because of the lack of an information technology connection, cases involving theft of personally identifiable information bore some resemblance to cash drawer theft. The primary difference was that these PII thieves raided information systems instead of cash drawers and that personally identifiable information was the commodity of value. Given the large market for stolen user and account credentials that can be used to encode a credit card or automated teller machine (ATM) card for immediate use, personally identifiable information is only slightly less liquid an asset than cash.

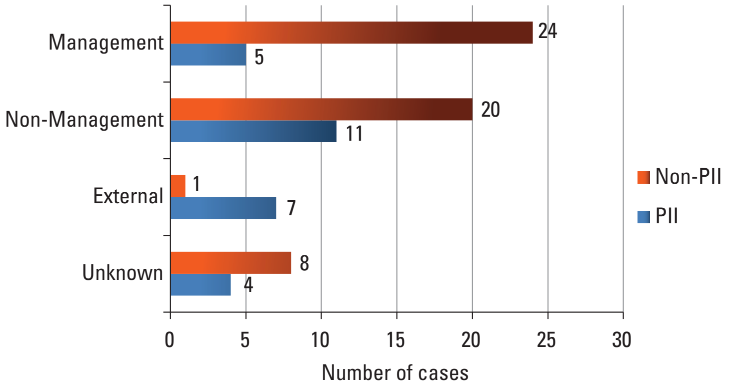
Switching Deposit Bags

Phil, a temporary bank employee, was responsible for processing large cash deposits and placing them in the vault in bank-issued deposit bags. On site and during work hours, Phil created counterfeit deposit bags using the company-issued system, put them in the vault in place of legitimate deposit bags, and stole the money from the legitimate deposit bags. In total, during a three-month period, Phil stole 12 deposit bags containing more than $92,000. Even though each of the 12 customers complained of their deposits not being credited to their accounts, it was not until the 12th customer's complaint that the organization conducted an investigation. Using surveillance footage and transaction logs, the organization discovered Phil's scheme.

Stealing cash from a drawer yields the insider immediate and tangible benefits, but it also leaves a clear trail that offenders must cover. Compared to cash drawer theft, the trail of evidence in inappropriate use of personally identifiable information may not always be as clear. The insider may have merely completed a normal activity (e.g., printing customer records) and used its outcome to profit externally. In every case involving personally identifiable information, the insiders had to export the data to a format that was acceptable to those who ultimately consumed the personally identifiable information.

Some insiders used creative methods of exporting data to avoid detection. In several cases, audits of the subject's information system usage revealed that the subject had violated policy, though it was not clear if the audit was random or not. Because the audit trail for personally identifiable information is more difficult to trace, financial institutions must restrict insiders' ability to indiscriminately access and export it.

Because personally identifiable information is such a sensitive and critical organizational resource, to better understand this type of crime, this analysis includes all cases of fraud committed by subjects both internal and external to the organization. Of the 80 cases, 34 percent involved personally identifiable information and 66 percent did not. The external cases were evenly split between personally identifiable information cases and non-personally identifiable information cases.



Crimes involving personally identifiable information are committed by younger, less experienced employees.

Though monetary damages are only one measure of a crime's severity, actual monetary damages in the two categories of cases (i.e., personally identifiable information and non-personally identifiable information) were compared in the study. As with other findings and analysis, there are several cases with extremely high damages that skew the numbers when calculating the average; therefore, the median was also computed. For cases involving personally identifiable information, the average damage per case was $222,896 and the median damage was $52,339.

The non-personally identifiable information cases involved damages roughly four times as large, both for the average ($1,046,670) and the median ($186,000). That might suggest that the personally identifiable information cases were insignificant or not worthy of concern. However, 10 personally identifiable information cases involved damages that exceeded $100,000, and 2 involved damages of more than one million dollars.

A potential explanation for the lower damages of personally identifiable information cases is that they were detected and stopped earlier than non-personally identifiable information cases. These cases included several crimes of unknown duration in both categories, which reduced the number of cases with known duration to 18 personally identifiable information cases and 43 non-personally identifiable information cases.

The crimes involving personally identifiable information were consistently shorter in duration. The median durations were 6 months for personally identifiable information cases and 19 months for non-personally identifiable information cases. The averages were much closer, at 19 months for personally identifiable information cases and 27 months for non-personally identifiable information cases.

Even when accounting for the long duration, personally identifiable information cases bringing the average up, more than 80 percent of the subjects committing crimes involving personally identifiable information did so for less than two years before being caught. Perhaps the detection mechanisms worked better in these cases, or perhaps these criminals were not as good at concealing their crimes. No matter the explanation, these cases still caused significant financial damage and potentially exposed organizations to unwanted consequences, such as disclosure requirements and potential regulatory penalties and fines.

Issuing Fraudulent Credit Cards

Ed, Jessica, and Lee were customer service employees at a financial institution's call center. They had access to customer information, which included personally identifiable information. While accessing customer accounts during the normal course of business, Ed, Jessica, and Lee printed computer screens that displayed customer records and gave them to an outsider to make fraudulent purchases. Sometimes they modified customer records to have a credit card sent to an address to which they had access, and they would use these newly issued fraudulent cards to make fraudulent purchases. Jessica even purchased a wedding dress with a fraudulent card. The organization's total losses exceeded $2.2 million.

The characteristics of employees who committed acts of fraud with personally identifiable information included the following:

- Age—The average age of subjects (at the beginning of the crime) who misused personally identifiable information was 32 years, while subjects who did not use personally identifiable information were, on average, 40 years old. Though there were 16 cases with unknown ages and several subjects on the extreme ends of the age scale, the median values are similar to the averages: 30 years for personally identifiable information cases and 40 years for non-personally identifiable information cases. Clearly, those who used personally identifiable information in the commission of their crimes were more likely to be closer to entry into the workforce than on the road to retirement.
- Tenure—Consistent with the finding about age, the subjects who were involved with personally identifiable information crimes had not been with the organization as long as non-personally identifiable information subjects. Personally identifiable information subjects spent an average of less than 8 years (7.5 years) with their organization before being fired for their actions. Non-personally identifiable information subjects had spent, on average, over 11 years (11.2) with the organization.
- Level of Seniority—Personally identifiable information cases involved both managers and non-managers, but the number of non-managers involved with trafficking personally identifiable information was more than twice the number of managers.

Table 2: Comparison of Crimes by Their Involvement of Personally Identifiable Information

	Crimes Involving Personally Identifiable Information	Crimes Not Involving Personally Identifiable Information
Age	32 years	40 years
Tenure	7.5 years	11.2 years
Position of Seniority (unknowns excluded from calculated percentages)	Managers—22% Non-managers—48% External Parties—30%	Managers—53% Non-managers—44% External Parties—2%

Taken together, these variables paint a fairly consistent picture of insiders committing crimes involving personally identifiable information—such crimes tend to be committed by younger, less experienced, non-managers. The crimes involving personally identifiable information were also caught more quickly than non-personally identifiable information crimes and, on average, resulted in less damage. However, some personally identifiable information crimes caused damages as large as non-personally identifiable information crimes, so the potential financial impact of these crimes should not be ignored.

INSIDERS WHO COMMIT FRAUD

The research team discovered two main probable scenario types (manager and non-manager) and developed system dynamics models for each. More information on these models is available in the insider threat study, *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector,* available at www.cert.org/insider_threat/.

Managers

A manager who commits fraud in a financial services organization typically has these characteristics:

Is a branch manager or vice president

Is motivated by financial gain to resolve a personal problem

Does not end the crime, even after the financial problem is resolved

Commits fraudulent activities over a 33 month period

Has the ability to alter business processes, including influencing subordinate employees

Experiences unexplained financial gain

Has subordinates contribute unknowingly to fraud activities

May be suspected by subordinates because of making irregular requests of them

Has a significant period of loyal service to the organization before attempting the fraud

Is generally considered trustworthy by others in the organization

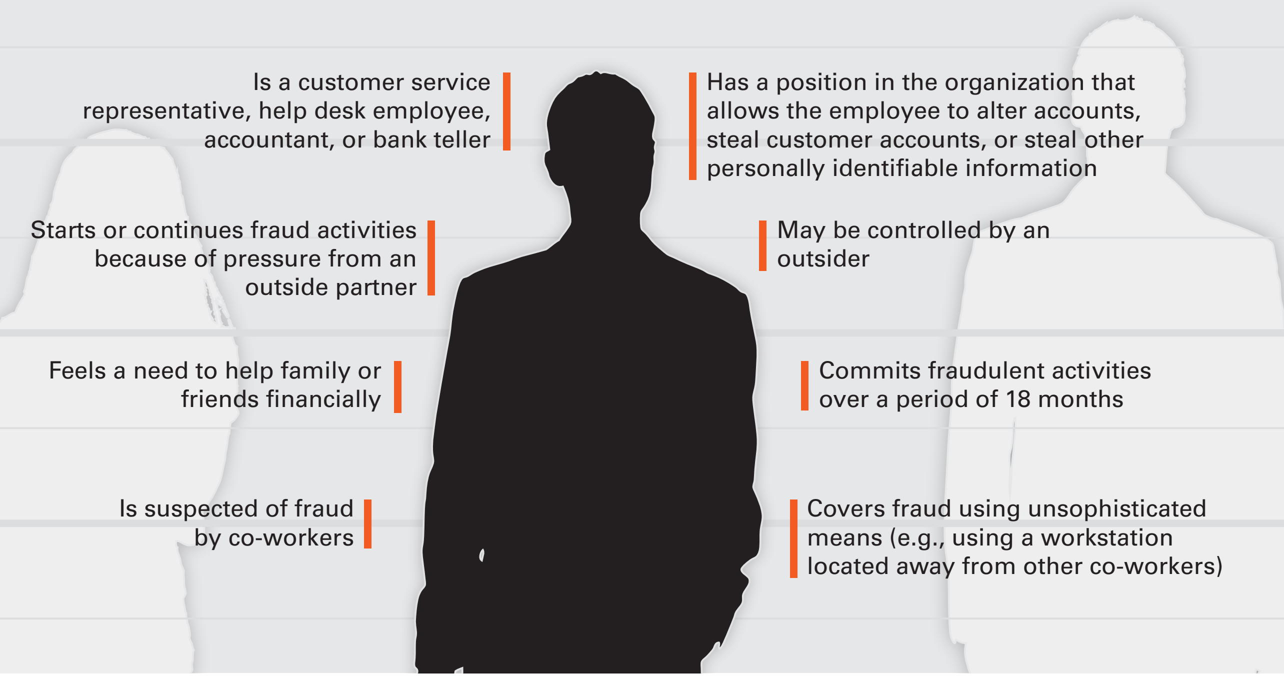
Uses the organization's trust to do one or more of the following:

- disables fraud-detection controls
- disables fraud-prevention controls
- increases privileges to gain knowledge of potential weaknesses in the organization's fraud-control system
- leads coworkers to ignore or fail to report behaviors considered policy violations

May ensure that the per-month fraud losses are low to avoid detection

Non-Managers

A non-manager who commits fraud in a financial services organization typically has these characteristics:



- Is a customer service representative, help desk employee, accountant, or bank teller
- Has a position in the organization that allows the employee to alter accounts, steal customer accounts, or steal other personally identifiable information
- Starts or continues fraud activities because of pressure from an outside partner
- May be controlled by an outsider
- Feels a need to help family or friends financially
- Commits fraudulent activities over a period of 18 months
- Is suspected of fraud by co-workers
- Covers fraud using unsophisticated means (e.g., using a workstation located away from other co-workers)

WHAT YOU CAN DO

Arm yourself with knowledge by getting a complete copy of the insider threat study, *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector,* which is available at www.cert.org/insider_threat/. The CERT Common Sense Guide to the Prevention and Detection of Insider Threats may also provide useful guidance for addressing the wide range of threats posed by insiders.

The following strategies can be inferred from the findings of the research study. These strategies are fairly general in nature, but are the start of what we hope will be a fruitful discussion with organizations to elaborate what members of the financial services community should do in the face of these findings. These strategies should be implemented with other organizational controls targeted at preventing, detecting, or responding to malicious insider activity. Be sure to consult with legal counsel prior to implementing these strategies or any organizational controls to ensure their compliance with federal, state, and local laws.

1. Clearly document and consistently enforce policies and controls.

Consistently enforce policies because inconsistently enforcing policies may lead some employees to feel that they are being treated differently than other employees, which may provide a potential motivation to retaliate against this perceived unfairness.

2. Institute periodic security awareness training for all employees.

Security awareness training helps employees be aware of security policies and procedures, the reason they exist, that they must be enforced, how to report policy violations, and the serious consequences for violating them. Employees also need to be aware that others may try to co-opt them into activities that are counter to the organization's mission, including committing fraud.

3. Include unexplained financial gain in any periodic reinvestigations of employees.

Institute a periodic reinvestigation of employees to determine whether employees are under significant financial stress, exhibit unexplained wealth, or are living beyond their means to identify those who are more likely to participate in fraud.

4. Log, monitor, and audit employee online actions.

Enforce account and password policies and procedures to associate online actions with the employees who performed them. Use logging, periodic monitoring, and auditing to discover and investigate suspicious insider actions early. Use data-leakage tools to detect unauthorized changes to systems and the download of confidential or sensitive information, such as intellectual property, customer or client data, and PII.

5. Pay special attention to accountants and managers.

Separate employee duties into critical business processes to prevent fraudulent transactions from occurring and institute audit programs to identify when fraud might be taking place. To protect against auditor involvement in fraud, consider implementing processes that "check the checker." Finally, ensure that the auditing function is unpredictable in terms of schedule, frequency, and what is audited.

6. Restrict access to personally identifiable information.

Do not allow employees to accumulate privileges over time from moving across projects, between departments, or from taking new positions. Ensure that employee privileges are necessary for their current job responsibilities. Protect PII from unauthorized access and establish controls that alert the proper personnel when PII is accessed, modified, or transmitted.

7. Develop an insider incident response plan.

Develop an insider incident response plan to control the damage that results from malicious insider activity. Ensure that only those responsible for carrying out the plan understand and are trained on its execution. If an insider is suspected of committing fraud, ensure there is evidence in hand to identify the insider and follow up appropriately.

SHARE YOUR EXPERIENCES

The Insider Threat Center welcomes ongoing feedback on practices and technical solutions that you have implemented in the financial services sector to successfully counter insider threats. The center also collaborates with organizations to research related topics. Contact the Insider Threat Center at insider-threat-feedback@cert.org.

A MESSAGE FROM THE DEPARTMENT OF HOMELAND SECURITY

Cyber crimes committed by malicious insiders are among the most significant threats to networked systems and data. When developing policies and procedures for responding to cyber security events, it is important to consider the insider threat.

A malicious insider is a trusted insider who abuses his trust to disrupt operations, corrupt data, exfiltrate sensitive information, or compromise an IT system, causing loss or damage. Left unchecked, their rogue actions may compromise the nation's ability to fend off future attacks and safeguard critical infrastructure assets, such as the electric power grid. In fact, some of the most damaging attacks against the government have been launched by trusted insiders. As increased information sharing exposes sensitive information to more insiders, such attacks will become an increasingly serious threat.

The research described in this booklet was sponsored by the Department of Homeland Security Science and Technology Directorate's Homeland Security Advanced Research Projects Agency Cyber Security Division. This booklet was derived from the 2012 report *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*. The work was conducted, and the report written, by members of the CERT® Insider Threat Center at Carnegie Mellon University's Software Engineering Institute. The authors built upon a previous S&T-funded 2004 report, *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,* to develop a greater understanding of the behavioral, technical, and organizational factors that lead to insider threat attacks. Drawing on case files provided by the United States Secret Service, they analyzed actual incidents of insider fraud, from inception to prosecution. As part of their effort, the authors compared the technical security controls commonly used to prevent internal and external attackers. Their findings can be used to inform risk management decisions being made by government and industry and to support law enforcement in cybercrime investigations.

I would like to specifically recognize the tremendous participation by the United States Secret Service in this effort. In granting the authors access to case files, the agency was instrumental in the development of this report.

Douglas Maughan, Director
Cyber Security Division
Homeland Security Advanced Research Projects Agency
Science and Technology Directorate
Department of Homeland Security

CERT

Software Engineering Institute

Carnegie Mellon