

A First Data White Paper

Four Evolving Fraud Threats You Cannot Afford to Ignore

By:
Beth Summers
Director, Fraud and Risk Product Management

Introduction

For today's consumers, merchants, and financial institutions, fraud is inevitable. It's no longer a matter of "if" you will be affected—it's a matter of "when" you will be affected. Even with state-of-the-art detection and prevention mechanisms in place, the likelihood of being victimized by fraud or a security breach is alarmingly high. In fact, the Ponemon Institute found that 90 percent of businesses had fallen victim to at least one security breach during the 12-month period from June 2010 through June 2011, making the threat from cyber attacks a near certainty.ⁱ

Why is fraud so pervasive? It's simple: because it's highly profitable. While the rest of the world economy continues to languish, fraud has become a multi-billion dollar industry—and malicious activity is growing at a record pace. The global cost of fraud and identity theft is estimated to be over \$200 billion per year—including \$54 billion in losses to businesses and individuals in the United States.ⁱⁱ

Worse yet, today's criminals are more sophisticated than ever, and are always on the lookout for new ways to exploit vulnerabilities in the payment system. For example, in 2010 improved fraud prevention practices resulted in a decline of the misuse of existing credit card numbers. However, during the same period, the rate of new account fraud remained steady. Because new account fraud is often harder to detect and results in a longer period of misuse, fraudsters simply adapted to the evolving marketplace.ⁱⁱⁱ

The Insidious Reach of Fraud

According to the Identity Theft Resource Center, at least 662 significant data breaches in the U.S. occurred in 2010, compromising more than 16 million records.^{iv} Nearly two-thirds of breaches exposed Social Security numbers, and 26 percent involved credit card or debit card data.^v The majority of these attacks were malicious hacks or insider theft. The Privacy Rights Clearinghouse reports that security breaches have compromised more than 542 million U.S. records since 2005, and those are just the reported incidents.^{vi}

Data breaches are constantly in the news, and recent high profile cases show that no organization is immune. Here are a couple of noteworthy examples:

Epsilon Data Breach Exposes Millions of Email Addresses^{vii}—In April 2011, the servers of the largest distributor of permission-based email in the world, Epsilon, were attacked by hackers. The attack revealed millions of individual email addresses. As the largest permission-based marketer in the world, Epsilon sends more than 40 billion marketing emails per year on behalf of its 2,500-plus major clients.

For this type of attack, phishing is the number one concern. With email addresses affiliated with Epsilon's customers in hand, cybercriminals could easily send fake emails pretending to be a consumer's bank, pharmacy, or any other company associated with Epsilon. The email would look real and would be convincing, as attackers have the customer's name and the company information they did business with. The email could ask unsuspecting users to click on a link that would ask for credit card numbers, run malware, install spyware, or carry out other attacks.

Sony Hit Hard by Cyber Attack^{viii}—Following on the heels of the Epsilon breach, Sony suffered a massive breach in its video game network, which included both its PlayStation Network and Sony Online Entertainment service. More than 101 million gamers had their data compromised including names, email addresses, and passwords. At first, it appeared that there was no evidence of credit or debit card information being stolen. However, after further investigation, it was found that the bank account information for 10,700 customers in Europe was stolen.

Even without evidence of stolen credit card information, the breach was troubling to security experts because many Sony gamers were likely to have used the same passwords for email and social networking accounts. The hackers could resell the user name and password combinations to other criminals, who could take control of those accounts and mine them for bank account passwords or to send bogus emails to friends' addresses to infect them with spyware or malware.

Four Evolving Fraud Threats

It cannot be stated too strongly: today's criminals are sophisticated and organized, and are continuously refining their methods in order to keep pace with emerging channels of delivery, new customer behaviors, and technology advances. With a low probability of being caught or prosecuted, the risk-reward tradeoff for fraud is extremely attractive.

Fraudsters are always on the lookout for ways to exploit vulnerabilities in the payments system with the goal of stealing funds by accessing consumer accounts. Financial institutions may not be the direct target of all fraudulent activities, but in the end, they bear much of the eventual cost.

While it is impossible to anticipate or prevent every attack, one way to stay a step ahead of these criminals is to have a thorough understanding of the different types of attacks and how the business of fraud is evolving. Here we explore the top four categories of fraud and data compromise, what risks they bring, and how criminals are changing their tactics. With this understanding, those affected by fraud have a better chance of mitigating the risks and stopping criminals in their tracks.

1. Network Intrusion

Network intrusion is a malicious activity conducted on a network by hackers or others attempting to misuse or break into a system with the intent of stealing data. It represents the majority of fraud that takes place today. The number of identities exposed due to hacking is more than three times that of other methods of attack.^{ix}

Network intrusion covers a range of attack methods, including:

- **Malware**—Comprises a variety of forms of hostile, intrusive, or annoying software or program code that can collect sensitive information from a computer, undetected. Spyware, botnets, and keystroke logging are all forms of malware.
- **SQL injections**—Involves entering SQL code into web forms such as login fields or browser address fields to access and manipulate the database behind the site or system. In other words, it tries to fake out the login function using SQL commands instead of actual user names and passwords to gain access to sensitive information
- **PIN hacking**—On the low-tech side, some criminals use cameras to record customers entering their PINs. More sophisticated criminals grab unencrypted PINs while they sit in memory on bank systems during the authorization process, or tap into a bank's hardware security model (HSM) and trick the HSM into providing an encryption key to "unlock" the data passing through the system.
- **Packet sniffing**—With packet sniffing, a malicious intruder can capture and analyze all of the network traffic within a given network, and capture username and password information that is generally transmitted in clear text and viewable by analyzing the packets being transmitted.

What are the Evolving Challenges?

The sophistication level of these threats has increased and attackers are getting smarter about evading detection. The longer it takes for network intrusion to get noticed, the more information criminals can steal. They also have more time to use the stolen information before infections are discovered.

Many malicious programs, such as packet sniffing, are now designed specifically to expose confidential information that is stored on an infected computer, and that threat is growing. According to Symantec, 64 percent of potential infections were threats to confidential information, an increase from 58 percent in 2009.*

Once the account data is acquired, hackers can use social networks to find personal information that may provide answers to security questions or help imitate buying patterns that fool fraud detection systems. With the widespread use of online shopping and Internet banking, the potential for loss can be significant, forcing financial institutions to put more emphasis on authentication and to dedicate even more resources to detection and prevention.

2. Social Engineering

Social engineering is the manipulation of people, rather than hacking into computers to steal information. The key to social engineering fraud is to deceive a person into performing a particular action, such as revealing a password or account number.

Many of these attacks start with network intrusion in the form of stealing email addresses from a financial institution or other company. The criminals then send emails that link to a fake landing page mimicking the consumers' bank or credit card provider's site. The consumers enter usernames, passwords, Social Security numbers, and/or account information—unaware that a cyber thief is capturing that data for malicious use.

Another common social engineering practice is to send an email plea from a friend or relative asking for money or information. Criminals know it is hard to resist a request for money from a known friend who has "had their passport and wallet stolen" while in a foreign country.

What are the Evolving Challenges?

As stated previously, mobile devices are opening up new channels for fraud, and they are a perfect target for social engineering. Many financial institutions and other companies now send text and/or voicemail alerts to customers whose account balances are low or have payments due, and retailers often send text messages to customers to announce sales and promotions.

If fraudsters get their hands on customer mobile phone numbers, the customers become instant targets for SMiShing (text) or Vishing (voice)—fake alerts or messages that fool customers into revealing passwords or account numbers.

Fraudsters Like Social Media, Too

Unfortunately, social media such as Facebook, Twitter, and LinkedIn are making it easier for criminals to commit fraud. Generation Y thinks nothing of posting personal information, giving cybercriminals enough information to impersonate someone else. With information about the friends, families, and interests of the people whose data they have compromised, fraudsters have a better chance to mimic buying patterns or answer security questions, making their crimes more difficult to detect.

In addition to harvesting information, criminals are using social networks to spread worms and viruses that help them gain access to accounts. According to *The Risk of Social Networking*, a recent report from Symantec, attackers use social engineering tricks to post enticing messages on behalf of an infected user, such as pleas for financial assistance. Curious friends follow the link, and then get infected with malware and unknowingly spread the message further. With people willing to click on any link from those in their private network, it's easy for attacks to succeed.

Criminals are also increasingly using social network sites to share successful tactics with other fraud perpetrators, enabling innovative new methods of fraud to spread rapidly through underground communities of criminals. In this way, vast networks of loosely organized fraudsters can experiment with new techniques through trial and error—and when a tactic is found to be successful, it can instantly be shared among cyberthieves.

3. Skimming

Skimming is an advanced method of stealing card information by using a small electronic device (skimmer) to swipe and store victims' credit and debit card numbers. The theft takes place in an otherwise legitimate transaction at ATMs, gas pumps, restaurants, etc. Using skimming techniques, thieves can gather account information, PINs, and even CVV2 numbers.

What are the Evolving Challenges?

Skimming often involves the use of a hidden camera to record customers' PINs or phony keypads placed over real keypads to record keystrokes. For criminals, there is a risk in getting caught when going to retrieve the devices. The criminals are getting smarter, though. Now, using Bluetooth technology, they can sit in a nearby vehicle and remotely gather data instantaneously, with no need to retrieve the devices they install.

Criminals also are getting smarter about where they install the skimmers. Traditionally a device attached to unattended terminals, criminals are now leveraging their social engineering skills to get an accomplice to install skimming devices at valid, card present locations. For example, in August 2011, a fast-food cashier pleaded guilty to skimming hundreds of customers' credit or debit cards at the Norfolk (Virginia) Naval Station McDonalds. She admitted to being recruited by another conspirator who offered her \$10 for every card she swiped. The conspirator used the account information obtained by the woman to manufacture fraudulent credit and debit cards.^{xi}

Criminals are also deploying coordinated attacks to distract cashiers and swap legitimate POS terminals with compromised devices. In May 2011, the Michaels craft store chain reported that 80 stores in 20 states had been victimized by fraudsters who had replaced existing PIN pads with devices that stole customers account information.^{xii}

4. Insider Fraud

Insider fraud is a term assigned to a wide variety of criminal behavior perpetrated by a firm's own employees or contractors, and generally falls into three categories: theft from customers, theft from the firm, and abuse of position. It is a growing problem among financial institutions, according to Aite Group. More than half of the financial services firms surveyed attribute at least 5 percent of their total fraud losses to internal fraud, costing firms hundreds of millions of dollars collectively.^{xiii} In another survey, Celent found that approximately 60 percent of bank fraud cases where a data breach or theft of funds had occurred were the work of an insider.^{xiv} Unfortunately, employees and contractors who access financial institution systems during the course of work know the system better than anyone else and they are better positioned to exploit the systems' vulnerabilities.

What are the Evolving Challenges?

As with other forms of fraud, internal fraud is changing. Historically, employee fraud involved account skimming and other small-scale attacks that put money in the employee's pocket. Today, with access to the online fraud forums, employees can advertise and sell customers' personal and financial information and make money without stealing directly from accounts. In one recent example of this type of insider fraud, an employee at a large U.S. bank leaked personally-identifiable information for 300 customers to a ring of international criminals.^{xv} Ten million dollars was drained from customer accounts, and the Secret Service eventually arrested 95 suspects involved in the crime.

Financial institutions may unknowingly hire someone whose sole purpose is to steal data from the company. It is much easier to exploit vulnerabilities from the inside with information about systems and processes, rather than hack in blindly from the outside—and criminal organizations are increasingly attempting to infiltrate banks by getting their members hired as legitimate employees.

In the retail industry, knowledge of the IT systems is not even necessary in order to perpetrate insider fraud. For example, dishonest employees can simply activate gift cards/prepaid cards and distribute them to friends and co-conspirators to purchase merchandise. Stolen cards are difficult to track, so it is easy for criminals to get away with making purchases, which they can resell for cash.

Fight Fraud with Holistic Mitigation Strategies

Along with having an understanding of what criminals are doing to adapt their fraud practices to the market, it's critical for financial institutions to implement necessary strategies for fighting these evolving strategies. Here are some strategies for keeping sneak attacks under control:

Empower consumers and cardholders through education

Traditionally, fraud has been measured in terms of financial losses. If losses met a pre-determined threshold, then the institution had a "fraud problem." But increasingly, institutions are concerned about customer loyalty—the customer experience. To retain valuable customers and accounts, institutions must reduce the risk of fraud by investing more in detection and prevention—and then make customers aware of those extra investments. Security no longer should be considered a corporate secret; it's a competitive advantage to be marketed.

All customers need to receive education about the potential hazards of social media and the risks associated with mobile devices. In a recent survey from the Information Security Media Group, 67 percent of financial institutions said that customer education is the best way to prevent fraud. Education initiatives not only help prevent fraud, but also boost consumer trust in a financial institution.

Make fighting fraud an integral part of internal culture

The Information Security Media Group also reports that cross-channel fraud is a growing trend. Fraudsters are no longer targeting just ATMs or payment cards or checks—they're seeking to compromise customers in every way that institutions interact with them.

This is why financial institutions must have fraud awareness and prevention programs deployed across every department. For example, the Marketing group should know and understand how to monitor for suspicious behavior when promoting new debit/credit card programs. At the same time, the Fraud Prevention group needs to understand Marketing's customer acquisition goals, and not implement fraud controls that are too stringent for a program to succeed.

Human Resources must also be on high alert when hiring employees, even those whose jobs do not give them access to sensitive information. Financial institutions scrutinize applicants for new accounts with authentication tools, and must be willing (and able) to use those same tools to screen potential employees.

All financial institution employees should be trained to detect and prevent fraud, both external and internal. Institutions should also have a clear process for reporting suspected fraudulent activity.

On the Horizon: Mobile Threats

While the reports of fraud related to mobile devices remain relatively low, the threat continues to grow. As more users download and install third-party applications and use them for sensitive transactions, such as banking and shopping, the incentive for attackers to infiltrate mobile devices will increase.

Lookout Mobile Security, a company that makes smartphone apps that scan and detect malware, reports that between a half million and one million mobile users were affected by malware in the first half of 2011. A significant part of the problem comes from Web-based threats which operate across platforms, with 3 out of 10 mobile users likely to click on an unsafe link.^{xvii} In addition, as more retailers move into mobile commerce, they expose themselves and their customers to new fraud opportunities.

The sheer number of smart phones and other mobile devices make it worthwhile for cybercriminals to allocate resources to designing "fraud programs" for this channel. Another reason to fear mobile fraud? Anti-virus and anti-malware applications are not as mature on mobile devices as they are on computers, making them particularly vulnerable to attacks.

Use data analysis tools to get a 360-degree view of fraud

To be proactive about fraud prevention, it's important for financial institutions to understand the fraud that's happening in their own portfolios and keep on top of what is happening in the industry, as well. As mentioned before, fraudsters are tricky—so what appears to be a small risk within your own portfolio could turn into serious fraud when viewed from an industry-wide perspective.

For example, say you view a pattern in your portfolio and determine that it is low risk, such as a certain address change or a test transaction from a specific merchant. Then, you look in the industry and see that the same thing has happened in nine other financial institutions of your size, and you can identify that for each one of them, every time it happened it was fraud. With that information, you can go back to your own portfolio and flag all the accounts that match that pattern, or be alerted when that pattern does occur—as well as to put checks in place to prevent the fraud from happening entirely.

Know your customers' behavior

Generally, financial institutions use 20 to 50 different data points on the back end for authentication decisions. In today's environment, having the capability to see many more data points and translating that data into a real-time risk decisioning can make the difference between being the victim of fraud and stopping fraudster in their tracks.

With access to more data points, you will know that an online purchase, even if it is just one time, is atypical for the 75-year old woman who lives in a small community and has never shopped online. Using that data analysis point, not just on the back end for your findings, but up front for the authorization decision, is critical to reducing and preventing fraudulent activity.

And it doesn't end with blocking the authorization; you also need back-end tools that allow you to communicate effectively with cardholders to notify them about fraudulent activity, to reissue cards, and really take the proper action to mitigate fraud, while maintaining accountholders' faith in your brand.

Summary—Taking Preventive Measures

With attacks coming in many different forms and from many different channels, financial institutions must gain a better understanding of how criminals operate and how fraud is changing. With this understanding, you will have a better chance of mitigating the risks and recognizing attacks before they do serious damage.

In addition, financial institutions need to adjust fraud detection and prevention strategies to keep up with the evolving trends. In some cases this means investing in new technologies; in others, it means bridging organizational silos. In all cases, it means improving your odds of detecting a fraud threat before it reaches the customer.

Key elements of a fraud prevention strategy should include the following:

- Tools that help prevent credit and debit card fraud
- PCI compliance and transaction data protection solutions
- Innovative ways for detecting transaction fraud
- In-house and outsourcing options for managing fraud disputes
- State-of-the-art tools for verifying customer identity
- Data sources and predictive modeling that help mitigate risk
- A comprehensive set of options to help maximize collections

Ultimately, data security comes down to protecting the lifeblood of your business—your customer relationships, and the trust your customers place in you.

Sources

- ⁱ Ponemon Institute. "Perceptions about Network Security." June 2011.
- ⁱⁱ *Accenture Outlook*. "Cyber Security to Improve Corporate and National Defense." Paul O'Rourke and Matt Gollings. March 2011.
- ⁱⁱⁱ *SC Magazine*. "ID Fraud Incidents Decline in 2010, but Costs Go Up." Angela Moscaritolo. February 8, 2011.
- ^{iv} *InformationWeek*. "Hackers, Insiders Behind Most Identity Theft." Mathew J. Schwartz. January 4, 2011.
- ^v Ibid.
- ^{vi} <http://www.privacyrights.org/data-breach>. Accessed November 30, 2011.
- ^{vii} *PC World*. "Epsilon Data Breach." April 4, 2011.
- ^{viii} *Internet Retailer*. "Sony Data Breaches Highlight the Fraud Risks Online Retailers Face." May 3, 2011.
- ^{ix} Symantec Corporation. "Internet Security Threat Report, Vol. 16." 2011.
- ^x Ibid.
- ^{xi} www.fox43tv.com. "Cashier Admits to Skimming Credit Cards." August 5, 2011.
- ^{xii} Dark Reading. "Michaels Breach Evidence of Growing POS Skimming Trend." May 13, 2011.
- ^{xiii} Aite Group. "Internal Fraud: The Devil Within." 2011.
- ^{xiv} Bank Info Security. "Insider Threat: Tackling it with Technology." July, 2009.
- ^{xv} Bank Info Security. "Insider Fraud Suit: Example for Others?" November, 2011.
- ^{xvi} Information Security Media Group. "2010 Faces of Fraud Survey." 2010.
- ^{xvii} www.channelinsider.com. *Mobile Security Threat Rising: Report*. Nathan Eddy. August 4, 2011.



The Global Leader in Electronic Commerce

Around the world every day, First Data makes payment transactions secure, fast and easy for merchants, financial institutions and their customers. We leverage our unparalleled product portfolio and expertise to deliver processing solutions that drive customer revenue and profitability. Whether the payment is by debit or credit, gift card, check or mobile phone, online or at the point of sale, First Data helps you maximize value for your business.

About the Author

Beth Summers is Director of Fraud and Risk Product Management at First Data, where she focuses on developing new risk management products for financial institutions. Most recently, Summers led product development and deployment initiatives for enhanced fraud detection decisioning capabilities as well as for a new line of fraud trending and analytics. Summers also has led client product launch and optimization projects for First Data's fraud and risk product suite.

Summers participates in and leads many client-focused forums with an eye towards listening, interpreting and incorporating that client feedback into better processes and products for First Data's customers. She has eight years of experience in the industry and also serves as a subject matter expert for large internal and external initiatives, including regulatory, custom client consultations, and market assessment and analysis activities.

For more information, contact your First Data Representative or visit firstdata.com