Now You See It, Now You Don’t: A Review of Fraud Costs and Trends

Fraud is more dangerous to your business than you think, and treating it as a cost of doing business may be emboldening criminals and costing you customers. A well-designed fraud management program can help protect your customers and improve profitability.

By Krista Tedder
Product Owner, Risk Management and Fraud Solutions
Introduction: Is Fraud the Perfect Crime?
The very best crime, or the very worst, depending on your point of view, is the crime that goes unnoticed.

Imagine this: Today is your big day, and you are about to finalize an important contract. To seal the deal, you treat your customers to a fine lunch at a very special restaurant. You have an excellent meal during which you build on your relationship with your customers. When it comes time to pay the bill, you reach for your wallet. It’s not there!

How embarrassing is that? You are mortified as your customers watch you frantically search your pockets. Where could you possibly have lost your wallet? Of course, by the time you recall that someone bumped against you in the crowded lobby, your cash is gone, your cards are maxed out and the thief has vanished.

Now, imagine this same business luncheon once again. After a very successful meeting, you announce you’ll take the bill as you hand your debit card to the waiter. Moments later he returns and whispers that the card has been declined. How can this be? You have not used this card recently, and your paycheck was just deposited. You check—your card has not left your wallet. No one would have your PIN, would they? As your mind races to figure out what’s going on, one of your business associates asks, “Is there a problem?” You smile nervously and say, “No. No problem.” No problem indeed!

In today’s wired world, criminals are getting smarter. They no longer need to steal wallets to get your money. Instead, they infiltrate computer networks, watching for a weakness in security, waiting for a chance to steal information. They “phish” by sending bogus, yet seemingly credible e-mail messages asking unsuspecting victims for personal information. They tamper with credit and debit card readers to capture PIN and account numbers for counterfeit cards.

These thieves are modern-day pickpockets, leaving the scene before anyone realizes they’ve been robbed, escaping prosecution and looking for the next big opportunity. Unfortunately, unlike the one-on-one offense committed by traditional pickpockets, these cyber criminals strike on a much larger institutional scale, affecting millions of people in one fell swoop and costing businesses billions of dollars.
In fact, the Identity Theft Assistance Center (ITAC) says that security breaches are up 47 percent since 2004, with damages due to cybercrime costing approximately $100 billion annually and expected to increase. A consumer Web site that tracks and posts security breaches, InsideIDTheft.info, reports that in the last five years, approximately 500 million records containing personal identifying information of U.S. residents stored in government and corporate databases were either lost or stolen.

Cybercrime, security breaches, identity theft and just plain fraud are crimes of opportunity. The ubiquity of electronic payment transactions and the emergence of a global e-commerce economy offer criminals lots of opportunity to perpetrate fraud. Many criminals are emboldened by the anonymity of their actions, by businesses’ failure to recognize the many potential avenues for fraud and by the widespread acceptance of fraud as just another business expense.

So is fraud the perfect crime? Is there anything you can do to reduce vulnerabilities and build a stronger defense against fraud? This white paper explores how and why fraud happens, and it provides insight into the deeper elements of fraud and its repercussions. It also provides guidance on how to design a fraud prevention and detection program to better protect your customers and help grow your business.

Picking Your Business Pockets Is Big Business

Pickpockets scan crowds in search of the perfect victim: the one distracted by children, the one with her purse wide open, the one who just put his wallet in his coat pocket. Criminals take the same approach with businesses, watching and waiting for one with vulnerabilities and making a move when the time is right. Recent high-profile cases show that no one is immune to having their pockets picked—not even the big guys.

Processor Incident Breaks Card Theft Record – A major credit and debit card processing company reported in January 2009 that sometime during the previous year, unknown intruders planted malicious software to steal card data carried on the company’s networks. Given that the company processes more than 100 million card transactions per month, it is very possible that the number of compromised credit and debit cards is at least that much, if not more. Before this incident, a discount retailer breach in 2007, which involved the compromise of over 45 million cards, was the largest known breach. In late 2008, another payment processing company announced that its systems had been breached, resulting in the compromise of personal information belonging to approximately 1.5 million cardholders.

Industry watchers are suggesting that cybercriminals are now finding it more “efficient” to target card processors rather than individual retailers.

Supermarket Breach Raises Security Questions – Thieves hacked into an East Coast grocery store chain, stealing up to 4.2 million credit card account numbers and immediately using 1,800 of the numbers for fraudulent transactions. Under further investigation, it seems the thieves captured the data while it was in transit to banks for approval, representing the first large-scale piracy of card data in transit. Afterward, the company was found to be in compliance with security standards required by the Payment Card Industry, raising questions about whether the PCI standards are too ambiguous or not stringent enough to protect consumers. Within two days of the announcement, two class-action suits had been filed against the retailer on behalf of customers.

Meeting PCI compliance does not ensure that you are safe 365 days per year—constant monitoring and vigilance are required.

Bank’s Lost Tape Exposes Customer Data – Unencrypted backup tapes from a global financial services company disappeared after being sent to a storage facility. The missing tapes contained Social Security numbers and bank account information for 4.5 million customers. The tapes went missing in February 2008, but customers did not learn about the incident until May. In a separate incident in April 2008, a backup data-storage tape containing images of scanned checks and other documents relating to payments made to nearly 50 institutional clients went missing. In both instances, outside vendors were transporting the tapes.

When data is released to a third party, it becomes just as vulnerable as if it were in the hands of strangers. Make sure that the third party’s security is as good as or better than your own, and that the data is encrypted.

Mortgage Lender Encounters Insider Theft – A company employee systematically downloaded about 20,000 customer profiles per week onto flash drives over a two-year period before the FBI arrested him in August 2008. Working on Sunday nights when no one else was in the office, the thief, who was a senior financial analyst with the company, would take the spreadsheets to business center stores to e-mail to buyers. Over the two-year period, he sold the sensitive personal information of an estimated 2 million mortgage loan applicants.

Most businesses need to do a better job of monitoring employees. However, the threat of insider fraud becomes even greater in a bad economy as fearful employees look to cash in on valuable information in case they become unemployed.

These examples show that fraud is insidious and criminals have no reservations about when or whom they attack. More disturbing than this, though, is that the bank and retail victims of these crimes could unwittingly be enabling the criminals. How? By accepting fraud as an inevitable part of doing business and planning for it on the balance sheet, businesses create an environment in which they can absorb losses and “contain” the damage, improve security and move on. Criminals understand this completely.

There are other costs associated with fraud and cybercrime—costs that go beyond just the costs of the fraud itself, costs that are not so immediately visible on the balance sheet. As the criminals become bolder and more organized, these incidents can threaten the overall viability of a business.

So what are the real costs of fraud?
The Real Cost of the Perfect Crime

Let’s go back to that embarrassing day in the restaurant. After your debit card was declined, perhaps you called your bank to find out what was the matter. It turns out that the grocery store where you shop had a data breach, and cyberthieves managed to get your account number and PIN. The bank assures you it will send you a new card.

When the card arrives, you pause for a moment before activating it. Then, instead of putting the card in your wallet, you decide to play it safe and run that card through the shredder. For a little added assurance, you start shopping at a different grocery store. In that moment, both the card issuer and the grocery store lost a customer.

As it turns out, you would not be alone in your response to the incident. A Javelin Strategy and Research study shows that more than 30 percent of people affected by a data breach will terminate their relationship with the company that lost their information. The study also showed that consumers equally blame both their financial institution and the retailer that experienced the breach. In the consumers’ minds, blame is assigned at both ends of the transaction. This is an important part of the cost calculation that is often ignored by businesses.

Now You See It: The Direct Costs Associated with Fraud

There is no doubt fraud poses a persistent, direct financial threat to businesses and consumers, and the cost is going up.

→ In 2008, according to the 10th Annual CyberSource Survey, fraudsters stole a record $4 billion from online merchants, up from $3.7 billion in 2007. That’s a loss of 1.4 percent of online revenue to fraud, a rate that has held constant for three years.

→ The Ponemon Institute’s 2008 Annual Study: Cost of a Data Breach cites that data breaches cost companies an average of more than $6 million per breach, or $202 per record, an increase of 2.5 percent since 2007—not including the cost of notifying victims, which ranges from 80 cents to $1.40 per letter.

While the exact costs associated with payment fraud are difficult to pin down, it is clear that banks and merchants are burdened with enormous fraud-related expenses. For example, studies show that in 2007, bank losses totaled about $2.9 billion—with the largest share of losses associated with credit cards, followed by checks, debit cards and ACH payments. The high cost of preventing fraud and complying with regulatory and network security standards cost an additional $3.1 billion per year. During the same time frame, merchant fraud losses totaled about $15.6 billion per year, while their spending to prevent fraud reached $5 billion. Add it all up and the figures are staggering: $26.6 billion per year.

The potential for fraud-related loss is huge, so it is no wonder that businesses constantly focus on fighting the battle against fraud. But what happens when a breach does occur? Many tend to address the how and why it happened, turning their attention to operational issues to “fix the problem.” This approach often leaves the true victims of the crime, their customers, unaware of what happened until their card is declined unexpectedly. How businesses respond to fraud can mean the difference between losing or keeping their customers. So how are they doing?

4 Federal Reserve Bank of Kansas City, “Can Smart Cards Reduce Payments Fraud and Identity Theft?” September, 2008.
Now You Don’t: Loss in Consumer Confidence and Brand Integrity

Trust might be intangible and hard to quantify, but the result of breaking that trust is clear. A Ponemon Institute survey asked consumers affected by fraud about their level of satisfaction with the response and transparency of organizations that reported a data breach. The vast majority, 73 percent, were not satisfied. Fraud victims also report that their reaction to the crime includes spending less money, avoiding certain merchants, changing banks or credit unions and switching credit card companies—all of which equate to lower revenues for businesses.

Figure 1: Lost business continues to dominate the cost of a data breach, accounting for 69 percent of breach costs, up from 65 percent in 2007, while other costs continue to decline.

Following a data breach, organizations suffer from an increase in customer churn rates, including customers not even affected by the breach. In 2008, the churn rate after a breach was 3.6 percent, up from 2.7 in 2007. The increase indicates that customers are concerned about the impact of a data breach—concerned enough to discontinue their business relationship—and have not become desensitized by the frequent reporting of data breach incidents. Often unaccounted for in the “cost of fraud” equation are increased marketing costs related to convincing existing customers that the company is still “safe,” and the cost of acquiring new customers to replace the ones who left.

In these very tough economic times, businesses clearly cannot afford to lose customers due to a security breach. Although new data breaches are reported each week and seem to be getting larger in scope, consumers have not become indifferent or blasé about these occurrences. Regardless of who is at fault, victims are more likely to blame their financial institution for the breach, according to the Javelin study, and they believe it is primarily the financial institutions’ responsibility to protect them from breaches. They also are increasingly likely to terminate their business relationship due to lost data, producing consistently higher churn rates. Along with healthcare organizations, financial services companies have the highest average rate of churn following a breach (5.5 percent), reflecting the high expectation consumers have for the protection and privacy of their most sensitive data.

In light of the growing impact of fraud on profitability, consumer confidence and brand integrity, it is critical for businesses to understand how fraud happens and what to look for as criminals find ever more clever ways to do their work.

Easy Pickings – A Look at the Vulnerabilities

With the amount of personal data released through the Internet, the increasing use of debit and credit cards at the point-of-sale, and more sophisticated hacking tools, it is no wonder criminals jump at the chance to participate in what seems to be the perfect crime. First Data, a leader in payment processing and the operator of the STAR™ Debit & ATM Network, took a close look at 2008 debit fraud data for an insider’s view of vulnerabilities*. This has produced an interesting perspective on current fraudulent activities and insights into areas that could be of concern in the future.

Vulnerability #1 – Debit Card vs. Credit Card Fraud

Consumers suffer almost twice as many incidents of fraud associated with credit cards as they do with debit cards. Debit card fraud, however, causes consumers greater concern because only 88 percent of major banks provide guarantees for PIN debit fraud, while 100 percent guarantee against credit card fraud. In addition, consumers experience debit card fraud on a more personal level than credit card fraud because the stolen money is taken directly from their bank accounts. They worry about checks that will bounce, overdraft charges, non-sufficient funds (NSF) charges and even having enough money to cover their living expenses until the issue is resolved.

When debit card fraud occurs, counterfeit and stolen cards lead the way for the type of fraud most common with debit cards.

Figures 2-3: Fraud Type by Percentage

<table>
<thead>
<tr>
<th>Fraud Type By Percentage</th>
<th>Yearly Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterfeit</td>
<td>30.59%</td>
</tr>
<tr>
<td>Stolen</td>
<td>26.77%</td>
</tr>
<tr>
<td>Lost</td>
<td>14.53%</td>
</tr>
<tr>
<td>Card Not Present</td>
<td>12.82%</td>
</tr>
<tr>
<td>Fraudulent Application</td>
<td>11.43%</td>
</tr>
<tr>
<td>Account Takeover</td>
<td>3.72%</td>
</tr>
<tr>
<td>Multiple Sales Drafts</td>
<td>0.08%</td>
</tr>
<tr>
<td>Not Received</td>
<td>0.06%</td>
</tr>
</tbody>
</table>

The good news is that from January 2008 through August 2008, STAR issuers reported 30 percent less debit card fraud than during 2007, as shown in Figure 4 below. Increases in fraud toward the end of the year are attributed both to more financial institutions reporting fraud and to the major payment processor compromise event discussed earlier that affected numerous card issuers.

*First Data analysis of reported fraud transactions through the First Data debit networks, and reviews of individual financial institutions’ fraud rates. February 2009.
Vulnerability #2 – Certain Business Types and Geographies

Certain types of businesses are at a higher risk for fraud than others, and almost 25 percent of debit fraud transactions occurred within just three merchant categories: gas stations and service stations (14.5% of fraudulent debit card transactions, which is actually a decrease of 6% from 2007), discount stores (5.5%) and grocery stores (4.75%). Discount stores reported the highest average dollar loss, with the overall average dollar loss of reported fraud amounting to $304 per transaction.

While it intuitively makes sense that certain types of merchants are at a higher risk for fraud than others, it seems that when it comes to fraud, geography also plays a role in the risk factor. In 2008, California led the way for the top ten states—but many Internet merchants bill from there, thus artificially inflating the state’s percentage of fraud.

Figures 6: Percent of Total U.S. Debit Fraud by State

Relative to their populations, Florida, Illinois, Massachusetts and Connecticut reported particularly high levels of fraud, while Texas reported comparatively lower incidences of fraud. In general, the number of fraud incidents by state was closely related to population density and levels of commercial activity.
Vulnerability #3 – The Future of Fraud

Fundamental and rapid shifts are occurring in the debit card environment and the economy, spurring criminal behavior and creating a fraud environment that is more complex, organized and common than ever before.

→ **International Fraud** – A growing global economy has unfortunately stimulated cross-border fraud and financial crimes. Sophisticated crime rings are now plying their trade on a global scale using highly developed techniques. International cybercrime has highlighted a number of trends, ranging from the widespread availability and sale of tools that automate cybercrime to the rise of organized criminal networks that use phishing, spyware and other techniques to steal private account information. For example, the discount retailer breach in 2007 was the work of a Ukrainian hacker who caused losses of millions of dollars worldwide. He recently went to trial in Turkey for hacking several Turkish banks and was sentenced to 30 years in prison.

According to First Data’s analysis, international travel and entertainment fraud is on the rise, with international airline fraud having one of the highest dollar loss rates of all reported fraud types, at $2,460 per transaction. Some fraudulent transactions are as large as $20,000 or more. Fraud related to international services, technology and direct marketing are categories that also show increases.

→ **PIN Fraud** – While PINs go a long way toward protecting consumers from fraud, thieves will go to any length to gain access to PIN numbers. For example, PIN phishing is at its lowest rate since 2004, as consumers have learned to be on the lookout for fraudulent e-mails asking for them to reset their PIN prior to it expiring or for updating records. However, PIN SMiShing is on the rise, as criminals recognize the increased use of cell phones and mobile applications, such as mobile banking, and have replaced fake e-mails with fake SMS text messages.

In addition to trying to trick consumers into providing their PINs, criminals are increasingly tapping into the keypads where the PIN is entered, skimming the information right out from under the cardholders’ fingertips. Most PIN compromises take place at a POS pay-at-the-pump terminal, where it is more difficult to monitor people coming and going or to recognize tampering. The terminals being targeted are ones that have been in place for years and are scheduled for upgrades, including security upgrades. A California-based organized crime group travels across the country to add skimming devices to terminals, and is targeting several key states including Pennsylvania, Delaware, Rhode Island, North Carolina, Florida, Nevada, California, Washington and Oregon.

→ **Economic Hardship Fraud** – Bad times always bring a rise in crime, but this economic recession is setting the nation up for a wave of cybercrime. Experts warn that the broken economy, combined with increased online retail operations and ever-more sophisticated hackers, means data is more vulnerable than ever. Once information is stolen, it is sold to buyers who use this information to participate in a host of illegal credit fraud activities. As economic struggles continue, the demand for illegal credit information expands and the underground economy flourishes. In addition, as economic pressures mount, companies will also likely see dramatic increases in employee misuse of data, particularly from the computer-savvy middle-class. Economic hardship fraud brings an increase in all of the following:

- Deposit fraud and check kiting
- Non-sufficient funds with no intent to repay
- Identity theft
- False fraud claims – consumers stating fraud on their account when they were the ones who made the purchases
- Internal fraud

© 2009 First Data Corporation. All rights reserved.  firstdata.com
First Data’s analysis of fraud trends reinforces the notion that new types of fraud-related risk arise quickly as the U.S. and global economies continue to decline. But businesses must remain vigilant as fraud becomes so common that its occurrence is no longer remarkable, only its scale. By stepping up efforts to protect customers, businesses can let these modern-day pickpockets know that fraud is not the perfect crime while making an investment in future growth.

**Reduce Fraud and Grow Your Business**

Everyone sits up and takes notice when fraud occurs. When the supermarket hack compromised 45 million credit card accounts, people who never shopped there began to wonder if their preferred grocery store was safe. With the recent processor incident in the news, customers may begin to ask merchants what company processes their payments and may think twice about shopping with those merchants. Businesses can no longer deny that fraud and customer loyalty are inextricably linked.

Unfortunately, as indicated earlier, it seems that many organizations fall down on the job when it comes to notification and remediation of fraud. Consumers, particularly fraud victims, have strong opinions about how businesses should respond when a breach happens. Javelin’s research shows that consumers want:

- A general description of what happened
- A specific description of the personal information breached
- Information about what the business has done to prevent further unauthorized access
- Exactly what steps the business is taking to help victims, including a toll-free number and a personalized Web site
- Steps to take to prevent and detect fraud in the future

As illustrated in Figure 7, taking a proactive approach to prevention, detection and resolution gives businesses the opportunity to retain customers and even provide additional revenue-generating services. The fraud victims surveyed by the Ponemon Institute indicated that they found receiving free or subsidized services helpful, and of the customers that used the services, 48 percent remained more positive about the organization than those who did not receive services.

**Figure 7: Prevention-Detection-Resolution Model**

![Figure 7: Prevention-Detection-Resolution Model](image)

From the point of origination through the entire relationship lifecycle, businesses can find ways to protect consumer data while maintaining a positive relationship with customers. For example, ensuring that new customers get secure delivery of credit and debit cards can protect against identity theft and help create an image of a company that they can trust. Or having systems and processes in place that allow for timely notification and a positive interaction if a consumer experiences fraud will help maintain brand integrity and reduce losses related to customers terminating their relationship.

Remember the lunch scenario with your important client? With the proper notification process in place by either the merchant or the card issuer, it would likely have been a non-issue. And when your new card came in the mail, rather than shredding it, it would be back in your wallet for continued use.

By looking at fraud as a strategic business issue rather than another business expense, you have the opportunity to make headway against the criminals while gaining customer loyalty and growing your business.

Seven Ways to Improve Fraud Prevention, Detection and Resolution—and Customer Confidence

1. Year after year, the annual STAR consumer survey shows that customers value two things above all else when selecting a debit card to use: security and control. Consumers want to feel confident that their card issuer is adequately protecting their personal data and account information, and they want the ability to exercise control over their accounts. A strong risk management program can improve the brand and market share of an organization by elevating security (and customers’ perception of security) and providing extensive opportunities for individual control.

Currently, fraud identification is typically shared fifty-fifty: half the time the consumer identifies fraud and the other half the financial institution identifies fraud. Approximately 21 percent of the time that a consumer identifies fraud it is via paper statements; this percentage is too high considering the time required to send and receive statements. The subsequent duration of time provided to the criminal can inflict higher fraud loss rates and further damage brand integrity. By providing electronic options to consumers to monitor their own account, consumers will be empowered to protect their account. The following are options that provide consumers with control while potentially offering added security:

- Focus on Internet banking – Encouraging customers to look at their balances on a regular basis provides faster detection of fraud
- Go paperless – Reduces interception via mail or by someone the customer knows (over 30 percent of identity theft is perpetrated by someone the consumer knows), and reduces the need for shredding
- Consumer selected notifications – E-mail or text message notification for address changes, transactions and account changes provides another layer of defense
- PIN change options – Customer-specified designation of PIN change options (e.g., via the phone, at an ATM, online) maintains security and provides choice
- Card activation options – Providing options to automate or speak with an agent
- Account lock options – Customer options to “lock” their accounts from specific transaction types (all transactions, international, e-commerce, etc.). By providing authorization denial strategies to customers, financial institutions are “deputizing” their customers to maintain their accounts
- Interactive text message capability – Provides a process that will enable customers to confirm, before the authorization is approved, that the transaction is legitimate
- One-time use text password for online banking access – Provides customers the ability to authenticate that they are on the financial institution’s Web site and not being directed to a criminal Web site
Providing customers with a multitude of controllable options could reduce the overall fraud risk by more than 20 percent. If the consumer can identify the fraud as it is occurring, the window of opportunity for the criminal is reduced and the card can be immediately closed.

2. **Certain payment methods can also improve overall risk management efforts (as well as additional customer options).** Encouraging PIN transactions instead of signature transactions provides increased security. With the average PIN fraud loss at less than one basis point and signature debit fraud averaging over four basis points, financial institutions and merchants can benefit from increased PIN debit usage.

Providing mobile transaction options may also provide an increase in security. Consider this: If a consumer loses their card from their wallet, they recognize the loss in an average of eight hours. If a consumer loses their mobile phone, they recognize that it is missing in under four minutes. Again, timing is everything. One of the mobile technologies offered by First Data is the GO-Tag™ solution, which enables consumers to initiate a transaction with a sticker attached to their phone. The use of the RFID technology reduces the ability for criminals to skim the data and compromise the account.

Well-tested methods of securing e-commerce transactions are MasterCard Secure Code and Verified by VISA—solutions that require enrollment by the consumer for added security (they are inexpensive and provide added security benefits).

3. **How a financial institution handles data compromise events can also lead to significant gains or reductions in market share.** Over 70 percent of consumers believe that they should be notified of a data breach within the first seven days\(^9\). Due to the complexity of data integrity issues, in many instances the first several days are spent identifying what actions are required—additional monitoring or blocking—and reissuing some or all of the accounts. However, the greater the speed with which organizations can effectively communicate compromise events, the more likely the customer will remain a customer.

Immediate contact via phone has been proven to be the most cost-effective and efficient means of communication, and with e-mail follow-up, consumers can be provided with additional information. The communication should state what was compromised and the risks associated, provide details of the type of compromise (lost laptop, data intrusion, stolen tape, etc.) and provide details of what the organization is doing to prevent this from occurring again. Also providing a detailed list of options consumers have for monitoring their accounts (see item 1 above) has proven very effective in retaining customers. Additionally, education of staff is critical. The financial institution’s staff is the point of contact for customers and this is where the most misinformation is disseminated. By educating staff, a consistent and concise message can be communicated, preserving the brand and increasing confidence that the financial institution can protect customers’ data.

4. **The most underutilized program that complements risk management programs are card activation and usage campaigns.** Fraud often impacts inactive cards—and when this happens, the issuer loses its most effective detection mechanism: the customer. Inactive card fraud requires the financial institution to identify the fraud itself or wait for a statement cycle for the consumer to review the activity. But, if the customer is actually using the account and is actively enrolled in consumer monitoring tools, the odds of immediately detecting fraudulent transaction activity increases dramatically. Issuers can easily initiate “inactive-to-active” campaigns through the various automated tools now available. Campaigns can consist of explaining the benefits associated with the card, gift cards upon usage or increased rewards benefits. Consumers are also motivated by details of security features and account management choices available to them.

5. **Transaction monitoring using a neural network can be an extremely effective tool.** Fair Isaac’s model, currently utilized by First Data (FRIS and Falcon), is the industry-leading technology for fraudulent transaction identification and authorization decisioning. The ability to use cardholder behavior patterns, industry consortium and fraud pattern data, and rules strategies can help identify fraud the same day. Compare the following average detection intervals and per-card losses (based on First Data’s analysis of 2008 fraud data):

- **Issuers that did not use neural network technology** identified fraud within the first five authorizations
  - Loss per card was approximately $770
- **Issuers monitoring transactions with neural network technology** identified fraud within the first three authorizations
  - Loss per card was approximately $462

Additionally, if consumers are aware that the transactions are being monitored, then the number of transactions they initiate will generally increase. Average transaction rates for FRIS (First Data’s debit neural network product) increased an average of four transactions per month per account. Multiply the transaction totals by the number of cards and the interchange revenue associated, and fraud detection options could actually be profitable for a financial institution.

6. **Authentication is also becoming critical in the current environment.** The 2005 Federal Financial Institutions Examination Council (FFIEC) multi-factor authentication rules provide additional security, but it isn’t enough. Criminals are starting to focus their attention on spoofing (the act of mimicking) phone numbers to bypass verification of phone numbers on file. By adding authentication measures beyond phone number and Social Security number verification, criminals are forced to know more about the consumer than what can be stolen from a database, laptop or wallet.

   Authentication procedures that ask out-of-wallet questions that are not on file, and are not multiple choice, are critical. Standard “canned” authentication questions can also be broken because many institutions ask the same questions: Where did you go to elementary school, what city were you born in, etc. By asking the customer to select questions and provide answers, the data is stored in a database. If the data integrity is breached, the customer’s other accounts have a higher rate of compromise since many of the answers are the same. By implementing a more sophisticated authentication process that does not rely on the financial institution to maintain a database, consumer security increases dramatically. The process can also be more cost-effective for the financial institution—the same authentication process can be deployed in call centers, IVRs, and online.

7. **As economic conditions continue to deteriorate around the world, cash will be the primary target for criminals, and ATM security will continue to be a major priority.** Financial institutions must consider implementing enhanced ATM monitoring practices and technologies to prevent and detect increasingly common occurrences of ATM fraud. Measures include better tampering detection and notification, as well as analytic solutions that identify anomalies in ATM usage (e.g., detecting a criminal standing at a machine for a long time using multiple counterfeit cards to withdraw cash at a high velocity).
Conclusion

Fraud will continue to be a crime of opportunity and the thieves will continue to steal methodically from companies until those companies go out of business. But you can work to stop them in their tracks and turn their “perfect crime” into a big mistake. How? By refusing to accept fraud-related loss as simply a cost of doing business, and recognizing that fraud has a strategic impact on your business that costs you losses in brand integrity and customers. Creating and implementing a comprehensive fraud program that includes prevention, detection and resolution components not only will limit your losses, it will strengthen your business.

Fraud is a complex, continually evolving crime that often involves multiple sources and methods. Businesses must fight back with robust fraud mitigation strategies across multiple channels, and continue to develop and refine fraud controls to combat the ever-changing fraud landscape while providing consumers with tools and knowledge to prevent, detect and resolve fraud. Only then will businesses be able to protect customers and grow their businesses.
The Global Leader in Electronic Commerce

First Data is a recognized leader in the prepaid card industry, and has a dedicated team of industry and compliance professionals that deliver secure, successful market-leading prepaid solutions to customers of all sizes. For more information on First Data’s prepaid offerings, please visit:

About the Author

As product owner for Risk Management and Fraud Solutions for First Data, Krista Tedder is responsible for the development of risk management, fraud and collection solutions that meet the market challenges faced by financial institutions. During her tenure with First Data, Krista has consulted with financial institutions to mitigate risk exposure while improving cost control and customer relationship management. Prior to joining First Data, Krista spent five years with MBNA in various positions focused on risk management and fraud.

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