



Avoiding the Lightning Strike of Identity Fraud

Is your organization adequately protecting the personal data of your customers and employees?

By William A. Alford, CFE

The headlines scream warnings about the latest breaches of data security and the public is once again put on alert that their personal data may be in danger. Nightly news shows are featuring stories about high-tech thieves who hack into supposedly secure databases and steal credit card and personal information and then ruin credit histories of unsuspecting consumers.

Credit card companies and financial institutions are using the public's fear of identity fraud in their marketing materials to help promote their services. There are even major insurance companies who are offering "identity theft" insurance.

Such high-profile incidents have shaken many institutions and continue to highlight the need for increased vigilance and security with regards to electronic transactions and proper storage of personal data.

For businesses and consumers alike, avoiding identity fraud is like trying to avoid being hit by lightning. Just as there are precautions you should take in the event of a lightning storm, there are similar common sense precautions that should be taken to protect ourselves against identity fraud.

Recent Breaches of Personal Data

In each of the following examples, the companies assumed that adequate security measures were already in place to protect the personal data of their customers and their financial transactions.

Bank of America—A data tape containing the personal information for over 1.2 million federal workers, including 60 U.S. senators was lost during a commercial flight transporting the tape to a secure location. Bank of America was not sure whether the disk was lost or stolen, but does not believe any foul play occurred.

Citigroup—In June 2005, the retail finance division of Citigroup announced that a backup tape containing personal information on almost four million customers was missing. According to officials, United Parcel Service lost the tape on May 2, and CitiFinancial noticed the tape was missing on May 20. The tape contained social security numbers and transaction histories on both open and closed accounts at the bank's lending branches in the U.S. Citigroup said it had no reason to believe the tape was stolen.

DSW Shoe Warehouse—Between November 2004 and February 2005, thieves accessed the firm's internal databases and obtained 1.4 million credit card numbers and the names on those accounts. Though the company has worked with banks and credit card companies to contact about half of the customers who were affected, the Ohio Attorney General's office has filed suit against DSW to force them to contact the estimated one million-plus customers who were affected.

BJ's Wholesale Club—Last year, thieves stole thousands of credit card records from BJ's internal databases, which resulted in multiple lawsuits. Recently, BJ's settled a lawsuit by the Federal Trade Commission (FTC), and the affected financial institutions have filed against BJ's to recover damages. According to the FTC, BJ's failed to encrypt customer data when transmitted or stored on BJ's computers, kept the data in files accessible using default passwords, and ran insecure, insufficiently monitored wireless networks.

Choicepoint, Lexis/Nexis—These companies provide background and

credit screening services and maintain personal data for virtually every person in the United States. Early in 2005, both companies reported serious security breaches. Choicepoint was scammed by fraudsters who signed up as customers and then accessed over 100,000 records. Lexis/Nexis reported that unauthorized users breached the system fifty-nine times using stolen passwords, and grabbed data belonging to 278,000 people.

MasterCard—In June 2005, MasterCard reported that a security breach occurred at Tucson-based CardSystems Solutions, a third-party processor of payment card data. Unknown hackers gained access to more than forty million cards of all brands. The compromised transaction data was not supposed to be held by CardSystems. Once a transaction is processed, the card data is supposed to be deleted from their system. But ironically, CardSystems stored the data in order to carry out unauthorized research into why particular transactions had registered as unauthorized or uncompleted.

Personal Protection

Financial institutions, businesses, and law makers are frantically trying to address these threats to our privacy before more losses occur and consumer confidence in the security of financial transactions continues to deteriorate.

The FTC published a comprehensive report on identity theft and fraud in 2003. The report stated that identity theft cost consumers and businesses \$53 billion in 2002. However, according to the report, 63 percent of consumers who are the victim of identity fraud bore none of the cost or incurred any out-of-pocket expenses. Instead, businesses and financial institutions absorbed the cost of fraud. Although consumers "could" be held responsible for up to fifty dollars in unauthorized charges, the major card companies are touting their "zero liability policy," which states that consumers are no longer required to report fraudulent activity within two days and are not responsible for fraudulent transactions.

Even if the consumer does not incur out-of-pocket costs, the problems

associated with having their hard-earned credit rating hijacked can be felt for years afterwards. For example, if a social security number is stolen and abused, every financial transaction in the future will be questioned because social security numbers are assigned for life and cannot be changed.

The term *identity fraud* or *identity theft* is very broad, and there are many variations. When a young person obtains a fake ID to drink alcohol, he or she has committed identity fraud. When a terrorist obtains fake documents to enter the country illegally, that, too, is identity fraud.

However, the vast majority of identity fraud we see today involves the theft of current credit card information or the establishment of new credit accounts for the purposes of obtaining goods and services while someone else pays the bill.

There are numerous steps consumers can take to help avoid identity theft. You can find the following precautions listed in the popular literature on the subject.

- Don't routinely carry your social security card in your wallet, or any such card or identification that displays your social security number.
- Don't give out your social security number to businesses unless there is a legitimate need.
- Use a shredder to destroy all sensitive documents, such as credit card offers and old bank statements.
- Reduce unsolicited credit card offers by using an "opt out service."
- Minimize the number of credit cards you carry.
- Scrutinize credit card statements each month for unauthorized charges.
- Regularly obtain a copy of your credit file for suspicious or unauthorized credit activity.
- Do not give out personal information over the phone to telemarketers or anyone that you do not know.
- Do not give out personal information over the Internet or in response to email solicitations even when such emails appear legitimate.
- Don't put bills, checks, and other such items in your mailbox for pick up. Instead, take to them to the post office or use a U.S. Postal Service drop box.

However, even with the heightened awareness of how individuals can protect themselves, identity fraud continues to be the fastest growing crime today according to the FBI, Secret Service, and every other laws enforcement agency in the country. Crooks and fraudsters have learned that stealing someone's credit history or using their credit cards is the ultimate high reward/low risk crime.

As a society, we have been very liberal with the sharing and warehousing of personal information in the past. The problem is, "Once the bell has been rung, it can not be un-rung."

- For example, until recently several states still use a person's social security number as their driver's license number, while others record it on applications and store it in their database.
- Many insurance companies use patient's social security number as the patient ID number and print the number boldly on the insurance card.
- Universities and colleges routinely use the social security number as student ID numbers. They also use temps and other students to enter mounds of such data during the registration period, making this an ever more vulnerable process.
- The neighborhood retail and service businesses that we use, such as exercise clubs and video rental stores, have been asking for and receiving personal information for many years. While most no longer ask for social security numbers or credit card numbers, many still have all of the customer applications "on file" at the stores and usually anyone in the store has access to the files.

Like the chance of being hit by lightning, the chance of becoming a victim of identity fraud is still slim statistically speaking. Yet, as the storm gathers and lightning strikes increase, so too does your chance of getting a hit.

The Business Impact of Identity Fraud

According to a report by the Government Accounting Office (GAO), 75 percent of the time, victims of identity fraud never know where or how the thieves got their personal information.

Take, for example, the many cases of identity theft that are committed by clerks or employees of doctors' offices or retail stores where customers freely gave their social security number and other important information in order to obtain goods or services. Consumers are at the mercy of every business, governmental agency, medical establishment, and university who is in possession of their personal information.

Compounding the problem is the fact that the filing, maintenance, and retrieval of this personal information are usually performed by hourly wage clerical workers. Therefore, many of the common sense precautions outlined at the beginning of this article are rendered ineffective.

This author's earliest experience with identity fraud involved internal data theft at a major supermarket chain in Florida in 1985. A clerk stole hundreds of completed check-cashing card applications. With those, he was able to obtain credit card numbers, bank account numbers, social security numbers, addresses, and other

personal information. The clerk used the information to purchase thousands of dollars in merchandise. Ironically, the reason we collected personal information from customers before granting them a new check-cashing card was to prevent and deter fraudulent checks, another form of identity fraud that retailers have been battling for many years.

There are countless examples of such fraud and abuse within companies that do not involve the massive number of customers referenced early in the article. Instead, businesses will likely face problems of lesser magnitude created by their own employees abusing the personal data of their customers.

According to a 2003 study conducted by the University of Minnesota, it is estimated that 70 percent of all identity fraud cases originated with data obtained by company or organization insiders. Given the virus-like spread of identity fraud, companies must conduct detailed internal reviews of data security and

continued on page 58

Kiss Your Key Management Problems Good-bye!

Is your system:
Too costly to operate?
Too time consuming to manage?
Leaving your property and assets vulnerable?

The InstaKey Security System is the Answer:

- Re-key up to 12 times without removing cores or lock hardware.
- Patent restricted, serial numbered key blanks that can't be duplicated without authorization.
- Online key management that allows you to manage your overall program's performance with auditing and exception reporting.

Making key management simple.

INSTAKEY
Security System

1498 S. Lipan Street, Denver, CO 80223
303.761.9999 www.instakey.com



Circle 24 on advertiser information form

control procedures and develop a structured investigative response.

Following are two examples of identity fraud in the business sector.

Sprint PCS Mobile Phone Provider.

In 2002, a customer service clerk of Sprint PCS in Charlotte, North Carolina, stole credit card information from account holders and used the information to purchase goods and services for his own use. It is also believed that he sold customer data to others who used the information to open fraudulent accounts and obtain merchandise. Customers of Sprint who lived in Seattle were the first victims to alert the company of unauthorized charges to their credit card, although the clerk was actually based on the other side of the country.

According to a quick background check, this author learned that the employee had been fired from a major office supply chain and charged with theft and embezzlement the year prior to being hired by the mobile phone provider. At the time, Sprint performed criminal background checks on all new hires. However, they allowed employees to work on a probation basis until the results of the background check were completed. This process sometimes took weeks, during which the company allowed these probation employees access to the "keys of the kingdom." Sprint has since changed their hiring practices and does not allow anyone to begin work until the criminal background check is completed.

The outcome of the case was typical for such cases of white-collar crime. The employee paid \$201 court cost, restitution in the amount \$2,634.29 and was placed on supervised probation for eighteen months. While anyone who has ever been a victim of credit card or identity fraud can attest, the impact of the employee's actions can affect the victim's credit history for years. Since this case is believed to also have involved the selling of customer data to other criminals, the victims' problems could grow exponentially.

National Medical/Health Provider.

(Provider asked that their name be withheld.) Two individuals named Jack and Jill worked at a doctor's office as

patient care representatives completing pre-testing of patients and preparing them to see the doctor. Because they were involved in the final checkout process for patients and collecting payments, they had direct contact with patient files. The patient files contained information about patient's medical conditions and personal information, including date of birth, social security numbers, and even credit card information. According to HIPPA, the Health Information Privacy and Portability Act, this is classified as PHI, or personal health information, which is protected from disclosure without the patient's knowledge or consent.

Jack was terminated for performance and attendance issues. Jack remained good friends with Jill. Jack asked Jill to give him patients' files, so she copied the contents of the files and smuggled them out of the office for Jack.

A few weeks later, a patient phoned the doctor to say he had received notice that a credit check had been performed on him, and he did not know who completed it. The customer had recently visited the medical offices and had a suspicion that the credit inquiry involved the medical office staff, but had no facts or proof.

Loss prevention was notified and the regional LP manager began an investigation starting with the employees who most recently handled the patient's records and worked with him during his office visit. The investigation led to Jill.

By this time, the medical offices had received a call from a second patient who had incurred unauthorized charges on a credit card that she rarely used. The only place she used that particular card that month was at the medical offices. This investigation also uncovered a link to Jill.

After reviewing all the files that Jill had worked with over the course of a month and watching her behavior at work, Jill was interviewed. She confessed to the fraudulent credit card charge and to making copies of patient files for ex-associate Jack. Jill said she wasn't sure what Jack was doing with the files, but she figured he was up to no good.

The police were brought into the investigation at that point and acquired a

warrant for Jack, who was identified as a member of a gang. Jack was arrested and his car confiscated. The car was a brand new BMW that was purchased with a loan taken out in the name of the male patient who originally complained about the credit report. In the trunk of the car were DVDs, CDs, CD players, and approximately twenty patient files that Jill had passed to Jack. Jack was also charged with theft of \$400,000, which he had stolen directly from the bank accounts of patients or by opening fraudulent credit card accounts in their names.

Shortly after this investigation, the state in which the case occurred began to seriously consider a law that if a business or medical entity learns that its patient's public health information has been compromised, the organization must inform those patients affected.

Protection Measures for Business

If the analogy holds true that the individual consumer is as unable to prevent identity theft as they are in preventing a lightning strike, what is the implication for businesses and those entrusted with private customer data?

Organizations have deep pockets and when fraud occurs can become the lightning rod for lawsuits and civil actions. Organizations must diligently secure critical information, such as social security numbers, dates of birth, and other personal data.

Take a close look at your company's operation and think like an identity thief.

Do you conduct criminal background check on all employees, even clerical workers, before they can begin work? Many companies only perform criminal and credit checks on management-level employees or those in financial or money-handling positions. Worse yet, they allow the person to work while the background check is being performed.

When making hiring decisions based upon criminal checks, do you include traffic and moving violations? A blanket disregard for such information may eliminate the people that have been charged with providing false information

to police, or have multiple names and addresses. These types of violations, while considered minor by many companies, are "red flags" with regards to potential identity fraud behavior.

If your customer records are computerized, are they password protected and does each employee have their own password? Is sensitive customer data segregated from more routine customer account information? Are there audit trails or reports for unauthorized or frequent access and are those reports being reviewed by someone on a regular basis?

A perfect example of how these controls can prevent an identity fraud nightmare involved an AOL employee who sold hundreds of thousands of email addresses to spammers. An audit trail helped investigators identify the source of the illegal access. Additionally, AOL wisely kept the database of email addresses separate from account holder information. By maintaining separate databases, the email addresses were sold, but the actual personal information of the account holders was protected.

In the event of a computer breach of a sensitive database, do you have a plan to notify affected individuals in a timely manner? California law dictates the time frame in which companies must notify their customers after a potential breach of personal information is discovered. Many states are rushing to adopt the same type of legislation. In any case, the question of disclosure of a potential incident should be discussed with your corporate attorney prior to an actual identity fraud incident with the understanding that each incident may be different and require different responses.

If sensitive customer and employee records are not computerized, are the records kept in locked cabinets or rooms where access is restricted? While performing a security survey for a large supermarket chain, I noted that they had excellent controls on their employee records, which were in large filing cabinets in a secured room manned by an employee who checked files in and out. However, right down the hall, the customer frequent shopper applications were left out on the desks of the data-entry personnel in a high-traffic area of the building.

Are you unnecessarily collecting social security numbers or other information from customers? If your organization must collect social security numbers, are they encrypted or truncated on your system or only accessible via passcode or PIN? Organizations need to be extremely cautious about collecting, using, and disclosing social security numbers of customers or other individuals. If lists of persons' social security numbers are available within an organization, employees can be bribed or corrupted to sell them, or can misuse them themselves.

A national fitness organization listed a place on their member application for social security number. After many questions by customers as to why they needed such information, the organization reprinted all of their applications. However, they did not want to waste the large number of existing applications so they allowed them to be depleted before rolling out the new applications. I personally observed a customer service clerk being berated by a customer who did not wish to give out their social security number. The clerk did not know that the organization was changing the applications and did not need the social security

continued on page 60

That Was
Then,
1975
Tape Based CCTV Recording

Featuring Proven
Optional POS
Integration

2005

This Is
Now.
21st Century
DIGITAL DATACATCH®

In 1975, VHS brought a new picture to security systems. But things have changed a lot since then. *Today*, what you want is digital technology. *Today*, what you want is **DIGITAL DATACATCH®.**

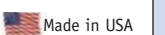
DIGITAL DATACATCH® uniquely features:

- Proven optional POS Integration
- Continuous recording capability
- 8 frames per second — continuously and simultaneously— up to 128 cameras
- 2800:1 video compression ratio
- More video, with any size hard drive
- Each camera input processed separately—no multiplexing or frame-sharing



5713 Industry Lane, Suite 56
Frederick, MD 21704

301-668-9440 • www.digitaldatacatch.com



number until she went to her supervisor to calm the customer.

Are shredders used in your offices and stores to destroy work documents that may contain personal information of customers and employees? A branch office of a state law enforcement agency experienced an identity fraud epidemic with many employees of the agency having credit cards obtained in their names. An investigation revealed that the work-release inmates who cleaned the building and emptied the trash each night may have been responsible for the rash of identity fraud cases in the office. So proves the cliché, "One man's trash is another man's treasure."

If you send statements, account documents, or invoices to customers, is the social security number listed on the document? Such personal information should be truncated to prevent authorized viewing. (Truncation is masking of most of the number with only a few of the numbers revealed.) The identity theft law of 2002 addresses truncation and mandates that such measures be taken to help prevent identity fraud.

If you accept credit cards, is the account number truncated on all sales receipts? Effective July 1, 2003, all Visa/MasterCard terminals should have been upgraded with truncating capabilities. The penalties for failing to truncate can be expensive:

- 1st violation - \$5,000
- 2nd violation - \$10,000
- 3rd violation - \$25,000
- 4th violation - \$50,000
- Willful or egregious violation - \$500,000 per month

In addition, there are federal and state penalties that may be levied. State

penalties vary, but can be up to \$10,000 per transaction and have felony charges associated with them. One dissatisfied customer or credit card company agent can report an establishment that is not truncating, and the business can be penalized or shut down, and the merchant may be placed on the Terminated Merchant File of Visa/MasterCard.

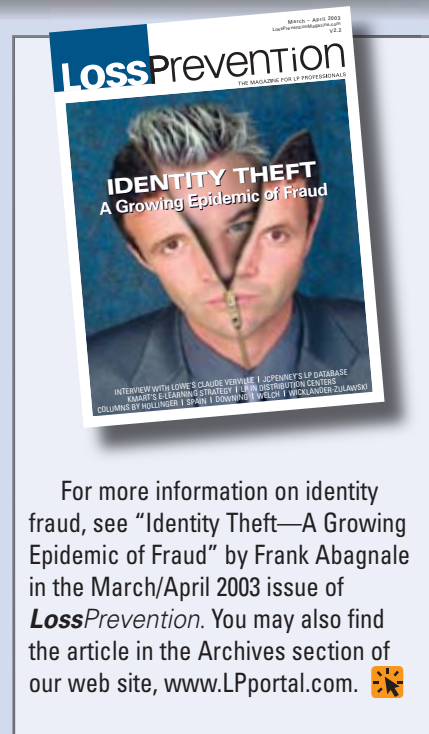
On phone or Internet credit card orders, are purchasers required to give you the authorization code number off the back of the credit card? This step stops a great deal of fraud where crooks obtain the credit card number and expiration date, but do not have the actual card. Next time you purchase merchandise over the phone or on the Internet, see if the company asks for this authorization number. Better yet, test your own company's phone and Internet sales policy to determine if they have this simple, but effective level of security in place.


If you use time cards, do they have the employee's name, social security number, and date of birth printed on them? Are they in a rack in a public place? Personal data should not be on the time card even if kept in the employee break area because other employees can use the data.

Are customer applications for credit cards, store charge cards, check cashing cards, and frequent shopper cards secured once they have been received? Such information should be handled securely from receipt from the customer to processing and final storage.

Businesses Must Take Notice

Federal and state lawmakers are proposing and enacting new laws, police are arresting the thieves, and, all the



For more information on identity fraud, see "Identity Theft—A Growing Epidemic of Fraud" by Frank Abagnale in the March/April 2003 issue of *Loss Prevention*. You may also find the article in the Archives section of our web site, www.LPportal.com. 

while, identity fraud continues to escalate in terms of the number of incidents, the magnitude of individual instances, as well as the overall financial burden on businesses.

Lawmakers such as Rep. John Carter of Texas are considering legislation that would punish companies and organizations for failure to protect personal data.

We can also expect to see a new wave of civil lawsuits in the near future against businesses that fail to strengthen their internal controls that allow identity thieves access to personal data of employees and customers.

This being the case, it behooves retailers and loss prevention professionals to take proactive steps to protect consumers, employees, and the corporation. Don't let your company be a lightning rod for identity fraud. ■



WILLIAM A. ALFORD, CFE is president of International Lighthouse Group, a consulting company specializing in the creation and implementation of fraud prevention and loss prevention programs for organizations across the country. Prior to establishing his consulting business, he held LP management positions with several major retailers over a twenty-year period. Alford is a certified

fraud examiner, a member of the Association for Practical and Professional Ethics, and the 2005 chair of the Retail Loss Prevention Council of ASIS International. He is also a frequent speaker before state, national, and international organizations and trade groups. Alford can be reached at 704-841-7759 or balford@ilbgroup.com.

Tired of Playing Cat & Mouse Games?



I.B.T. Video works closely with today's loss prevention professionals. As the direct manufacturer, I.B.T. has the ability to incorporate customized features that will assist in day to day activities to enhance and maximize security measures. By putting customer needs and service above all, I.B.T. has built many long-term relationships with businesses across the country.

DVSR1000 Professional Class DVR

- POS interfacing for up to 16 POS devices per system.
- POS event search feature.
- 4-32 video inputs per system.
- Up to 240 frames per second record/display.
- Smart search technology.
- Advanced MPEG4 compression for DVD quality images.
- TV output for public view monitor.
- Easy to use interface.



Reliable...Built To The Highest Quality Standards



866-IBT-VID1
866-428-8431
IBTVIDEOSYSTEMS.COM

Contact a representative today for a complete list of our products and services.