

# DATA IN DANGER



## With digital age, customer identities are more vulnerable than ever

*By Bill Morrow*

An estimated 10 million Americans are affected by identity theft-related fraud every year, according to the U.S. Federal Trade Commission. As the number of criminal acts and people affected continue to rise, it is no longer enough to simply monitor credit reports and shred billing statements to prevent identity theft. Through advances in technology, social networking and banking, your customers' identities are more vulnerable than ever.

In August, the leaders of the largest hacking and identity theft scheme in U.S. history were indicted after their plans to allegedly steal more than 130 million credit and debit cards were uncovered by authorities. The alleged leader of the crime had been in and out of the grasp of the Secret Service for allegations that he was the orchestrator of the 2003 T.J. Maxx data breach, stealing more than 40 million credit card numbers and costing the retail chain about \$200 million. Afterward, he acted as an informant for the Secret Service before returning to commit even bolder crimes.

The magnitude of these recent crimes is clear proof that the security of personal information is always in jeopardy. For businesses that collect or maintain customers' personal information – as banks do with Social Security numbers, credit card numbers and bank account numbers – such news enforces the importance of educating customers about how they can keep identity thieves at bay.

### **A network of identity thieves**

Social media is the latest resource identity thieves have hacked into to find unsuspecting victims. When signing up for a social networking site, users are commonly asked to provide their name, address, telephone numbers, date of birth, schools they have attended and places of employment, among other things.

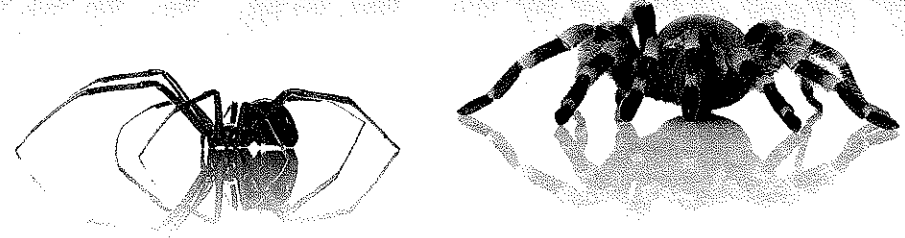
Many of the security questions asked by banks and other institutions can be answered with the information now posted on the Internet for anyone to see.

Criminals also obtain the details they need to steal a person's identity by engaging in "friendly" conversations with a potential victim, which involves discreetly asking questions

that often lead to the exchange of personal information. This is known as "social engineering."

Keeping as little information as possible on these sites is the best way for your customers to protect against identity theft. One piece of information on one site can be combined with other facts found online to make it easier to steal a person's identity.

# DATA IN DANGER



## With digital age, customer identities are more vulnerable than ever

By Bill Morrow

An estimated 10 million Americans are affected by identity theft-related fraud every year, according to the U.S. Federal Trade Commission. As the number of criminal acts and people affected continue to rise, it is no longer enough to simply monitor credit reports and shred billing statements to prevent identity theft. Through advances in technology, social networking and banking, your customers' identities are more vulnerable than ever.

In August, the leaders of the largest hacking and identity theft scheme in U.S. history were indicted after their plans to allegedly steal more than 130 million credit and debit cards were uncovered by authorities. The alleged leader of the crime had been in and out of the grasp of the Secret Service for allegations that he was the orchestrator of the 2003 T.J. Maxx data breach, stealing more than 40 million credit card numbers and costing the retail chain about \$200 million. Afterward, he acted as an informant for the Secret Service before returning to commit even bolder crimes.

The magnitude of these recent crimes is clear proof that the security of personal information is always in jeopardy. For businesses that collect or maintain customers' personal information — as banks do with Social Security numbers, credit card numbers and bank account numbers — such news enforces the importance of educating customers about how they can keep identity thieves at bay.

### A network of identity thieves

Social media is the latest resource identity thieves have hacked into to find unsuspecting victims. When signing up for a social networking site, users are commonly asked to provide their name, address, telephone numbers, date of birth, schools they have attended and places of employment, among other things.

Many of the security questions asked by banks and other institutions can be answered with the information now posted on the Internet for anyone to see.

Criminals also obtain the details they need to steal a person's identity by engaging in "friendly" conversations with a potential victim, which involves discreetly asking questions

that often lead to the exchange of personal information. This is known as "social engineering."

Keeping as little information as possible on these sites is the best way for your customers to protect against identity theft. One piece of information on one site can be combined with other facts found online to make it easier to steal a person's identity.

### Be safe when online

As banks focus their services on convenient Internet and mobile applications, it is important for customers to protect their personal information online. First off, advise your customers to use unique logins and passwords for each Web site. For example, if your password is "bluefox09" for your e-mail account, do not use it or a small variation of it, like "bluefox10," for your bank account password. This way, if one account is breached, the other accounts will be less at risk. Also, never use information related to the actual account (i.e., don't include your bank account number in your password).

If a customer believes his/her identity or personal information has been compromised, recommend resetting all accounts and selecting secure passwords that include letters, numbers and symbols, which are harder for hackers to crack.

### Phishing for information

Scammers "phish" for information by sending spam e-mails or pop-up messages under the name of a financial institution or similar company to gain people's trust and convince them to reveal personal and financial information. Often, in the form of an e-mail from a bank or credit card company, the message will claim there is a problem with your account and, by replying with your password, the financial institution will be able to fix everything.

Remind customers to never to e-mail personal or financial information and to always use your secure online application to verify account information. Also, once an e-mail scam is reported by one of your customers, it is important to notify all customers that an identity thief is attempting to access their information. This puts everyone on alert, making it less likely that they will fall victim to this scam. It is also important to constantly remind customers of typical online safety practices like not opening e-mail

attachments from non-trustworthy sources, entering financial information on non-secure Web sites (look for "https" in the address) or downloading files from non-secure sites.

### Vishing over the phone

Vishing is the new phishing. Instead of asking consumers to click a link, identity thieves use Voice over Internet Protocol (VoIP) phones that recognize telephone keystrokes. The consumer receiving the call is told to call a regional phone number because his/her credit card has been breached. When the person calls the number given, another prompt asks for the consumer's 16-digit account number, PIN code, Social Security number and other personal information to verify the account.

Inform customers that even if they receive a phone call that appears to be from a trusted source according to caller ID, scammers may be using caller ID spoofing techniques to make the call appear as if it is from a legitimate phone number. Make sure customers are aware that their bank will never ask for login details on the phone, and if ever asked to do so, they should contact the company to check the authenticity of the call before replying.

### Skimming the details

Debit and credit cards have become staples in people's wallets and purses. Unfortunately, one swipe of the card may cost more than what is on the receipt. Skimming is the practice of stealing a debit or credit card number by using a special storage device to swipe the card to collect the name, number and expiration date off the card's magnetic stripe, giving the thief enough information to make a duplicate card. If a PIN-based debit card is skimmed, the scammer can make withdrawals in the cardholder's name, possibly draining the account completely.

A customer's PIN is also at risk when the person uses his/her card at an ATM machine. Remind your

customers to always be aware of people peeking over their shoulders trying to see the PIN as they type it in and cover the key pad when entering the number. Also, it's recommended that customers change their PIN on a regular basis. Remind customers to pay attention to details, like whether the credit card is run twice by a cashier or if there are problems inserting the debit card in the ATM card slot.

### The bigger picture

Unfortunately, even if all the tips and tricks are used to deter identity thieves, your personal information has already been exposed to thousands of computers, starting from the day you were born when the hospital recorded your name, date of birth, Social Security number and parents' names. This is more than enough information an identity thief needs to steal one's identity.

It is important to find an identity theft protection service that monitors for criminal activity 24 hours a day, seven days a week with comprehensive protection that goes beyond credit monitoring. To protect yourself and your customers against identity theft and identity fraud-related crimes, find a company that monitors credit reports, non-credit loans, public records, change of address notifications, criminal records and the Internet for misuse of your personal information. Only then can you keep identity thieves away and help protect yourself from becoming another name in the growing list of identity theft victims. ♦

*Bill Morrow is chairman of CSIIdentity, an Austin-based fraud detection and identity theft protection company that offers a comprehensive suite of business and personal security solutions targeting all aspects and victims of identity theft.*

