

Identity & Identity
Theft Fraud

Fighting Back

Written by aimpublications LLC

It's the fastest-growing crime in the United States, annually costing 9 million to 10 million victims — and the organizations with which they do business — more than \$50 billion. But companies that maintain and share personal data are doing plenty to prevent it. Here's how you — and your company — can help.

A few large-scale computer-based heists notwithstanding, identity theft remains chiefly a personal crime. Fully half of U.S. identity theft and the fraud resulting from it is committed by victims' family members, friends and neighbors, according to Javelin Strategy & Research's *2005 Identity Fraud Survey Report*.

"ID theft not only impacts individuals, but their employers as well," notes Thomas Chapman, chairman and chief executive officer of Equifax. "The process of cleaning up the damage caused by ID theft can lead to hours of lost productivity."

Yet, ID theft also remains a mostly low-tech crime. Less than 12% of the identity information used fraudulently was obtained online, the Javelin study indicates. More conventional methods — lost or stolen wallets, theft of paper mail, sticky-fingered family or friends — are not only far more common, accounting for upwards of 68% of ID thefts, but often result in higher losses than online ID crime.

Protecting Electronic Payments Works

Last year, for the first time ever, electronic payment transactions in the U.S. exceeded paper-based check payments, according to the *2004 Federal Reserve Payments Study*. So it's not surprising that the most prevalent form of identity fraud involves credit cards. Nevertheless, the percentage of identity fraud involving credit cards has dropped dramatically in the last couple of years — from 41% in 2002 to just 28% in 2004, according to the Federal Trade Commission (*National and State Trends in Fraud & Identity Theft, January-December 2004*).

Certainly, the efforts of the major credit card payment systems have helped. Visa, for instance, operates a global transaction processing network that provides better than 99.999% reliability while settling nearly 100 million transactions a day.

"Visa's approach," says Susanne Lyons, executive vice president and chief marketing officer for Visa USA, "has focused on developing layer upon layer of fraud tools and protec-

VISA SECURITY PROGRAM

A MULTI-LAYERED APPROACH TO PAYMENT CARD SECURITY.

Zero Liability:

Helps cover fraudulent purchases.

In the event of loss or theft, you will not be held responsible for purchases on your card that you did not make.

Continuous Monitoring:

Helps detect fraud.

Visa continually monitors your account for fraudulent activity.

ID Theft Assistance:

Helps access 24-hour support.

Visa provides access to a 24-hour hotline to help cardholders who have become victims of identity theft.

Verified by Visa:

Helps prevent online fraud.

A personal password you create helps assure that only you can use your card at participating online stores.

3-Digit Code:

Helps distinguish your card.

A unique 3-digit number on the back of your card helps to ensure that you are actually in possession of the card during phone and online transactions.



VISA.COM/SECURITY

tions, including Continuous Fraud Monitoring and ID Theft Assistance.”

The company’s neural network-based early warning systems, risk management tools, security policies and programs, use of smart-card technology and collaboration with other organizations (such as launching the Phish Report Network with Microsoft, eBay and Whole Security) add up: fraud now represents less than one-tenth of 1% of total Visa card volume.

“The ultimate protection for cardholders,” adds Lyons, “is our guarantee that they won’t be liable for fraudulent purchases.”

Preventing ID Theft & Fraud: The 10 Best Practices

Like all people who steal, identity thieves seek the easiest mark. Here are some steps to take to protect yourself against them:

What individuals can do. Despite companies’ efforts to protect sensitive data and transactions, most ID theft and fraud is uncovered by individual victims. Fortunately, there’s plenty that individuals can do to both prevent identity theft and fraud and detect it promptly should it happen to them:

△ **Go electronic.** This means checking financial statements online (at least once a week), paying bills online whenever possible, signing up for direct deposit of your paychecks, and canceling paper-based statements and bills.

Why: (1) Research points to paper records and mail as the source of many ID thefts, whereas the Internet is the vector in just a small fraction of cases. (2) Electronic detection of ID fraud is faster (18 days versus 114 for discovery via paper-based statements) and losses are lower.

△ **Use e-mail-based alerts to review your credit report and monitor account payments, withdrawals, transfers and low balances.**

Why: ID fraud committed via new accounts is tough to self-detect and usually costs victims more than fraud involving existing accounts. Equifax, for instance, offers services that track all three credit reporting agencies and send alerts about key changes within 24 hours.



△ **If you have no access to online accounts, review paper bank and credit card statements monthly and look out for missing bills or statements.**

△ **Shred sensitive paper documents as well as expired credit cards.**

△ **Pick up your paper mail promptly and put sensitive outgoing paper mail in a secure mailbox.**

△ **Protect sensitive information and documents from the prying eyes of family, friends, neighbors and domestic employees.** This includes PINs, passwords, bank statements, paper checks and Social Security cards.

△ **Do not carry identifying data — such as your Social Security number, PINs or passwords — in your wallet or pocketbook.**

Why: research indicates more ID theft occurs as a result of lost or stolen wallets than from any other cause.

△ **Report lost or stolen credit cards immediately and cancel any inactive credit card accounts.**

△ **Do not click on any Internet links in e-mail messages from financial institutions or other companies with which you do business; instead, type the address you already know into your browser to make online contact.**

Why: ID thieves using scams with fake but legitimate-looking Internet addresses are likely “phishing” for your personal data.

△ **Install and faithfully update fire-wall, anti-virus software and anti-spyware.** **Why:** this security software can protect your computer and the sensitive data residing on it from most criminal attacks.

As organizations of all types transition from paper-based to online record-

EQUIFAX

Protecting Employees, Customers ... and Yourself

With the increase in identity theft, Equifax has developed a series of programs and tools designed to help you proactively protect your credit standing.

Take Control of Your Credit is an Equifax free credit education program available in English and Spanish at www.mycrediteducation.com. Its monthly e-mail newsletter, available at Equifax.com, provides updates on managing and protecting your credit.

The free **Equifax Toolbar** helps protect against identity theft via phishing by warning consumers before they visit a fraudulent Web site.

Most important, Equifax offers comprehensive identity theft protection products that are best-in-class. Its premium service, **Equifax Credit Watch™ with 3-in-1 Monitoring**, alerts you within 24 hours of key changes to any of your three nationwide credit reports. This in-depth service provides online dispute guidance to clear up errant and/or fraudulent information.

Equifax also offers programs that help businesses protect their employees and their customers, including proactive value-added programs and emergency services in response to lost or stolen information.

www.equifax.com

EQUIFAX

Advertisement 4

keeping, there's much they can do to protect the sensitive personal data of employees and customers that has been entrusted to them:

△ *Store sensitive data in databases and data storage environments secured via defense-in-depth systems and techniques.* Be sure to secure all computer systems — including mobile devices like laptops and PDAs — that contain sensitive data.

△ *Store paper documents and microfiche in spaces that are secured and monitored.*

△ *Develop a comprehensive privacy policy that articulates how sensitive data should be collected and used.* This includes establishing a data collection policy based on the idea that you collect only the information unequivocally needed to do business — do you really require Social Security numbers or full birth dates? This also includes assigning roles and responsibilities, honing a response plan to deal with questions and complaints, and creating a crisis-management plan in the event of loss, theft or electronic breach.

△ *Pay as much attention to disposing of sensitive data as to collecting it.* Electronic files should be “wiped” using special software, disks and CDs should be destroyed, paper documents should be shredded using cross-cut shredders, and dumpsters should be locked and not publicly accessible.

△ *Develop a policy limiting display and disclosure of sensitive data on documents, badges, paychecks and timesheets.* Do not use Social Security numbers as any sort of personal identifier for any purpose.

△ *Carefully craft and execute an organizational security policy that establishes who is allowed access to sensitive data and under what conditions such access is allowed.* Access to sensitive data should be limited to a need-to-know basis, and penalties for unauthorized access or browsing should be strict and severe.

△ *Deploy systems that constantly monitor and audit your organization's collection and use of sensitive data.* Conduct unannounced spot checks and reward those who adhere to best practices.

△ *Check employee backgrounds.* This is especially important for those with access to sensitive information and those with access to areas where sensitive information resides (such as cleaners, contractors, temp workers).

△ *Undertake regular staff training in privacy and security policy and responsibilities.* Don't forget to include contractors and temps.

△ *If a security breach involving sensitive information occurs, notify affected customers and/or employees.* In compliance with California law (Civil Code 1798.29 and 1798.82-1798.84).



This doesn't have to be daunting — services are available to help organizations protect against identity theft and fraud. Equifax, for instance, provides solutions that authenticate identities online, automate online risk and fraud assessment and identity authentication, predict fraud potential, spot high-risk applicants who warrant further investigation and help companies comply with government screening regulations.

“In this day and age,” says Equifax's Chapman, “it's shocking that people believe ‘it won't happen to me.’” He advises vigilance for both individuals and organizations. “Being notified within 24 hours ... enables you to quickly and effectively respond to possible threats, minimizing or avoiding any serious damage.”

Written by [aimpublications LLC \(www.aimpublications.com\)](http://aimpublications.com), provider of analytic and editorial consulting about key business and technology issues and trends.

WEB DIRECTORY

EQUIFAX

www.equifax.com

VISA

www.visa.com/security