

# How to Plug the \$13 Billion Leak



**Identity theft** is the fastest growing crime in the United States, but neither you nor your company needs to join the list of victims.

**H**ave you invested more in data security than Bank of America? Is your security tighter than Ameritrade's? Are you less vulnerable than Time Warner? Do you feel luckier than Lexis-Nexis—or Wachovia, Commerce Bancorp, Polo Ralph Lauren, PNC Financial Services Group and DSW Shoe Warehouse?

You'd better hope so. Because every one of those organizations was a recent victim of security breaches in which information about large numbers of customers or employees was lost or stolen.

Identity theft is America's fastest growing crime, according to the U.S. Federal Trade Commission. Some 10 million U.S. adults were victims in 2005, with almost \$15 billion in losses, according to IT

research and analysis firm Gartner.

For businesses, the consequences can be chilling: high recovery costs, lost revenues, damaged reputation, eroded consumer and investor trust. "Enterprises bear the brunt of the financial losses"—about \$13 billion of last year's \$15 billion, says Avivah Litan, vice president and research director at Gartner. "And our research shows that both online shoppers and online banking customers are more reluctant to conduct business electronically because of identity theft."

What's needed, then, is a coherent strategy for fighting identity theft and its effects. By understanding the evolving threats, as well as the emerging tools and techniques to counteract them, business leaders and consumers can go a long way

toward mitigating the risks of this insidious crime.

## From Crime to Crimeware

Identity theft comes in many guises—from dumpster diving by low-tech burglars to keystroke logging by high-tech crime rings. A particularly pernicious form is phishing, in which e-mails that appear to come from legitimate businesses invite users to give up personal data such as passwords and account numbers. Some 1.2 million Americans lost \$930 million to phishing between May 2004 and May 2005, according to Gartner.

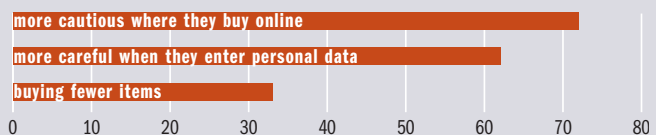
In addition, more than 80 percent of online consumers say they're less likely to trust e-mail from any company because of phishing. That has serious implications for companies that want to

### Taking a Toll on Consumer Confidence

Identity theft is making consumers alter their online shopping behavior, according to a May 2005 study of 5,000 U.S. adults who are online.

(% describing their attitude about buying online)

Source: Gartner



Special Advertising  
Section Sponsor



Reprinted from a Special Advertising Section appearing  
in the March 20, 2006, issue of BusinessWeek



reach customers by e-mail.

Even more threatening is the growing incidence of malicious software secretly planted on PCs. "Until recently, the worst attacks were from phishing," says Peter

### Signature Advice for Protection Against Check Washing

An increasingly alarming epidemic of a crime called "check washing" is giving rise to consumers and federal authorities nationwide. Some \$815 million is lost each year in the United States to this kind of fraud.

To help fight the crime, uni-ball® teamed up with Frank Abagnale, one of the most respected experts on identity theft and subject of the blockbuster movie "Catch Me If You Can." Together, they spread the word about how individuals can help protect themselves—it may be as simple as the pen you use.

Highly recommended by Abagnale for securing your signature, the uni-ball 207™ gel pen has ink that contains color pigments which are absorbed and "trapped" into paper fibers making check washing nearly impossible.

For more information and tips from Abagnale visit this Web site: <http://uniball-na.com>

Cassidy, secretary general of the Anti-Phishing Working Group. "Now we're seeing the rise of crimeware, which is much more serious, because it's automated."

Such "malware" can capture usernames, passwords and account numbers. It can also search PCs for confidential information—including corporate data—and transmit it to a criminal server.

What's more, each identity crime is no longer a small-ticket affair. "We're seeing

full-bore identity theft in which a criminal uses your identity to establish new lines of credit or even take out a mortgage," Cassidy says.

The good news is that security providers are offering a growing range of identity-focused products and services:

**Security utilities:** Includes traditional protections such as antivirus, antispam and firewall software. "Three years ago, 30 percent of viruses were designed to steal personal data," notes Vincent Weafer, senior director of Security Response at Symantec Corp., a provider of security products. "Today, it's 80 percent."

Good antivirus and antispam software can protect against up to 98 percent of attacks. But it's important to have all the bases covered with a comprehensive suite of products. "You can have the best antivirus software, but if you don't have a spam filter, you're still exposed," Weafer says.

**Strong authentication:** Identifies an individual by using two of three factors: something known such as a password, something possessed such as an ATM card, and something uniquely identifying such as a fingerprint.

Typically this is a matter of augmenting a password with a one-time-use scratch card, say, or a challenge/response approach in which a service rep asks a question that only the real customer can answer.

**Encryption:** Translates data into a secret code that's nearly impossible to decipher. Data can be encrypted inside a database or as it's transmitted over a network.

**Biometrics:** Uses a physical attribute—fingerprint, iris pattern, facial shape—

### For Identity Protection, Press Copy

New forms of identity theft seem to proliferate like copies on a photocopier. But perhaps none is more surprising than a modus operandi that involves copiers themselves.

Most organizations lease copiers from an office equipment dealer. When the copier comes off lease, the dealer typically re-leases it or sells it to a third party. "Now, criminals are buying these off-lease copiers," reports Mike Marusic, vice president of marketing for Sharp Document Solutions. "They read the data from the hard drive and sell the rest for parts."

In possession of a digital copier's hard drive, these data thieves can access the information it contains—customer data, trade secrets and more. "Copiers contain a company's most pertinent and up-to-date information," Marusic points out.

Sharp offers features that protect copiers and printers against unauthorized use, automatically encrypt and overwrite stored data, and restrict network connections only to authorized computers. "A growing percentage of our sales volume is from customers who want to protect the data on their copiers," Marusic says.

To learn more about how Sharp technology can reduce the threat of identity theft, visit this Web site for short and insightful white papers and other vital information:

<http://www.sharppusa.com/security>

to identify individuals. Laptops from major vendors such as IBM, Hewlett-Packard and Toshiba now come with fingerprint readers.

**Identity federation:** Provides access to multiple systems across departmental

### Preventing Identity Theft: 5 Consumer Tips

*Identity theft has no silver-bullet solution. Prevention requires a multipronged approach. Here are five ways your customers and employees can protect themselves.*

— 1 —

Don't carry your Social Security number with you, and don't give out your Social Security number except for tax, employment or credit purposes.

— 2 —

Delete any e-mail that asks for personal data or invites you to log into an account. If you think the e-mail is legitimate, call the company or access your account from outside the e-mail.

— 3 —

Provide your credit-card number only on secure Web pages, indicated by a closed padlock in the bottom right corner of your Web browser.

— 4 —

Use passwords that are at least six characters, use upper- and lowercase letters, combine letters and numbers, and don't contain your name or words that are in a dictionary. Don't use the same password for multiple accounts, and change your passwords every six months.

— 5 —

Get free access to one of your three credit reports every four months at 877-322-8228 or <http://www.annualcreditreport.com>.

and company boundaries. Users have a single secure identity that can be used once to access multiple services—logging in to a secure airline site, say, and then moving on to secure hotel and auto-rental sites without having to log in again.

**Transaction anomaly detection:** Uses rules-based software to monitor accounts and flag unusual activity—large funds transfers or repeated attempts to access an account, for example. The approach can work across multiple channels such as phone, ATM and Internet.

### Do What Works

Sometimes simple approaches are the best protection. A good example is uni-ball pens, some of which are specially designed to prevent a common form of check fraud. “Check washing” is a process in which fraudsters use common household products to erase ink from stolen checks and then make the checks payable to themselves. Losses from this type of fraud top \$800 million a year in the United States, according to uni-ball.

Specially designed uni-ball pens use inks that are absorbed into a check’s paper fibers and can thwart check washing. “Customer response has been overwhelmingly positive,” says Doug Kruep, senior brand manager for uni-ball. “This is a simple, inexpensive and effective way for consumers to protect themselves.”

Another common threat appears in the form of multifunction devices that combine printers, copiers and fax machines. Many users are unaware that digital printers and copiers store data on disk drives, just like PCs. Even if the data is deleted, it remains accessible on the disk until it’s overwritten by new data.

“One of the best times to steal identities is around April 15, when employees are using the company copier to copy their tax returns,” says Mike Marusic, vice president of marketing for Sharp Document Solutions. “Organizations invest in security to protect against outside intruders, but most identity theft occurs within the enterprise.”

Fortunately, manufacturers of multifunction devices are taking steps to secure their products. Sharp, for instance, offers features that protect devices against unauthorized use, automatically encrypt and overwrite stored data, and restrict network connections to only authorized computers.

### Beyond Technology

Like all data security, identity protection comes down to risk management—a balance between the need to protect data and the cost of doing so. Smart organizations have a comprehensive security policy and plan, an important component of which is identity protection.

Accountability for such a policy begins at the top. Consider designating a chief risk officer “with the ultimate responsibility for maintaining confidentiality of the data” along with “the requisite authority to carry out what is necessary to achieve this,” recommends Jonathan Penn, an analyst at Forrester Research.

A secure mindset must then extend throughout your organization. Human behavior is the most important aspect of identity theft. Employees must learn which company and personal data is confidential and which programs are acceptable for download.

Finally, invest in consumer-awareness

### New Book Offers Easy Ways to Keep You Safe

The Internet is crawling with risks. Even if you just surf the Web and send e-mail, you are exposed to hackers, thieves and con artists. Today’s bad guys don’t need to break your windows to invade your home—they can attack your family over the Internet. Are you prepared?

“The Symantec Guide to Home Internet Security” can help keep you safe while online. The book provides easy step-by-step help from Symantec, the world’s most trusted security provider, to help ward off Internet threats.

Written specifically for non-technical computer users, you’ll learn simple ways to be secure while online:

- Keep your PC free of spyware, adware, worms, viruses and intruders;
- Protect your identity and privacy;
- Eliminate junk mail from your inbox;
- Keep eavesdroppers out of your wireless network;
- Shield your children from pornography and online predators; and,
- Download free tools that help keep your computer safe.

Visit this Web site for more information:  
<http://www.symantec.com/idtheft>

campaigns, which Gartner’s Litan calls “one of the most effective tools for battling identity crimes.” After all, prompt discovery and reporting of identity theft can dramatically reduce monetary losses from fraud. ■

### Identity Theft Resources

To see an electronic version of this section ready for e-mailing to colleagues as well as links to analyst and association reports, case studies and other valuable information, please go to <http://www.businessweek.com/adsections> and click on the headline “How to Plug the \$13 Billion Leak.”

In addition, the Web site has hot links to the following organizations:

- InfoSecurity Canada Conference & Exhibition**..... <http://www.infosecuritycanada.com>
- Sharp Document Solutions** ..... <http://www.sharppusa.com/documents>
- Symantec Corp.**..... <http://www.symantec.com>
- uni-ball** ..... <http://uniball-na.com>

For more information on Special Advertising Section opportunities, please contact Stacy Sass McAnulty at 212-512-6296 or [stacy\\_sass-mcanulty@businessweek.com](mailto:stacy_sass-mcanulty@businessweek.com)  
 Please visit [www.businessweek.com/adsections](http://www.businessweek.com/adsections)

 **Triangle Publishing Services Co. Inc.**  
*The Best Strategic Content for Web, Print, Multimedia and Beyond*  
**[www.triangle-publishing.com](http://www.triangle-publishing.com) ■ 617-244-0698**  
 Special Advertising Section Writer: Eric Schoeniger  
 Designer: Carlson Webster Avery Advertising and Design