

From the April 18, 2005 print edition

Austin ranks 16th in identity theft claims; firms fight back

Jason W. Meeker
Contributing writer

It's 2:27 a.m. Do you know where your identity is?

Millions of Americans -- including Central Texans, of course -- are waking up to the realization that they can't always answer this question.

ChoicePoint Inc., an Alpharetta, Ga.-based provider of information for landlords and merchants who want to conduct background checks on potential tenants and customers, disclosed in February that con artists had duped the company into releasing personal data on more than 145,000 Americans.

Because we rely heavily on the digital transfer of messages, files, confidential information and even money, the specter of identity theft looms larger than ever. Just as unsettling is that businesses are finding the tactics used to steal a person's identity are being used to gain unauthorized access to sensitive and confidential corporate information.

Several companies in the Austin area are combatants in the fight against ID theft.

Austin-based WholeSecurity Inc. builds software to protect users of online services from identity theft. The software helps detect and lessen the effects of worms, Trojan horses, keystroke loggers and other eavesdropping programs for customers that include Comerica Bank, the Lower Colorado River Authority and eBay Inc.

WholeSecurity stresses the vulnerability of corporate networks that employees use remotely at home or on the road.

"Many companies allow their employees to have remote access. Using Trojan horses, home computers can be infected and monitored when an employee accesses corporate resources," says Oliver Schmelze, senior product manager at WholeSecurity.

"By stealing log-in credentials, passwords and user names, criminals can then break into a network and steal the online identity of that user. This also applies to online banking from home."

Online auction company eBay turned to WholeSecurity to help reduce its vulnerability to "phishing" attacks. Phishing is a tactic criminals use when they send fake emails to lure consumers to counterfeit Web sites, which trick consumers into providing credit card numbers, account user names, passwords or Social Security numbers.

The Austin area appears to be a hotbed for ID theft -- or at least awareness of it.

Last year, the Austin area ranked 16th among U.S. metropolitan areas for the number of per-capita complaints regarding identity theft, according to the Federal Trade Commission. Consumers from the Austin area lodged 1,417 complaints last year, or 113.4 for every 100,000 residents.

Across the state, an estimated 26,454 Texans filed complaints about identity theft last year. In March, Texas Attorney

General Greg Abbott urged Texas businesses that manage databases with sensitive personal information to "immediately undertake measures to ensure the security of the data."

A survey by the FTC indicates the U.S. economic impact of identity theft reached \$52.6 billion in 2004.

Infoglide Software Corp. is another Austin company working to reduce the economic toll of ID theft. Infoglide helps verify identities for government agencies and financial institutions. In 2003, Infoglide won a \$6 million contract from the U.S. Transportation Security Administration, which uses Infoglide software to validate identities and make risk assessments about travelers.

Infoglide's software contains a scoring system for conducting background checks, risk assessments, fraud detection, data mining, alias identification, market analysis and customer identification. Instead of transmitting sensitive data across networks, only a score is provided, which pinpoints whether an identity is authentic.

"We help you know your customer. So before you extend credit to somebody or move money into an account, we can help you know who that person and make sure they're not trying to defraud you," says Michael Torres, vice president of strategic marketing at Infoglide.

Managers at three Kroger grocery stores in College Station know exactly who their customers are, thanks to Round Rock-based Biometric Access Co.

Through the development of products such as thumbprint scanners, Biometric Access aids companies in verifying that people trying to buy products or access sensitive data are authorized to do so.

Under a pilot program using biometric thumbprint scanners, the three Kroger stores are testing the use of Biometric Access' SecureTouch Advance point-of-sale system.

Following an initial registration process, shoppers can use the system to check out by using their thumbprints -- instead of cash, checks or credit cards.

Rather than combating ID theft through software, Austin's Britestream Networks Inc. is ensuring data protection and privacy using hardware. Britestream's product embeds security features in hardware such as servers, routers and switches.

"The Internet was created with connectivity in mind. Security was an afterthought, so people find ways to hack into software. We're developing hardware solutions that businesses and consumers can use to protect their information," says Mike Salas, founder and vice president of marketing at Britestream.

Julie Ferguson, vice president of emerging technologies at Austin-based ClearCommerce Corp., is a leading voice in the battle against ID theft. She is chairwoman of the Merchant Risk Council, which seeks to establish e-commerce standards for merchants and to guard against fraud in online purchases.

ClearCommerce provides e-commerce fraud prevention and payment processing software for more 80,000 businesses around the world, including customers such as Apple Computer Inc. and Staples Inc.

Ferguson advises businesses and consumers to operate under the assumption that ID theft will happen.

"I advise a different tactic. I assume I am going to be compromised, and it's just a matter of when," Ferguson says.

"So what can I do to minimize the damage when my identity has been compromised? You should monitor your credit reports so you can minimize the damage once your identity has been compromised. Most people don't know their identity has been compromised for as long as six months."

Jason W. Meeker is a freelance writer.

