

October 15, 2000

Internet-aided identity thieves on prowl

Computers allow access to personal data, cloak criminals in anonymity

The Internet has increased the speed and scope of commerce, communication and research. But the same computer revolution that benefits citizens and businesses opens opportunities for criminals. With technology, the old crime of identity theft becomes easier.

- According to the General Accounting Office (GAO), a national credit bureau received 523,000 identity theft complaints in 1997, compared with 35,000 in 1992.
- The Social Security Administration reported 30,000 complaints about the misuse of Social Security numbers in 1999, up from fewer than 8,000 complaints in 1997.
- The Federal Trade Commission's Bureau of Consumer Protection has logged 20,000 calls in eight months on its identity-theft counseling hotline.
- A recent survey found that one in five households had experienced identity theft.

The Internet lets thieves obtain personal information and then cloaks their fraudulent activities in anonymity. In July, the director of the Bureau of Consumer Protection told a Senate Judiciary subcommittee hearing that "the fear of identity theft has gripped the public as few consumer issues have."

Identity theft also threatens businesses. The potential employee might not be who he or she claims to be, or might not have the credentials listed on the application. Fear of fraud might make consumers shy away from e-commerce. Businesses must take precautions to ensure that vendors are who they say they are.

The U.S. Department of Justice defines identity theft as a crime in which someone wrongfully obtains and fraudulently uses another person's personal data, usually for economic gain. Thieves use the personal information—address, date of birth, Social Security number—to get fake driver's licenses and credit cards. Identity theft also includes using fake credentials (like a police badge or a college diploma) to gain access or inflate accomplishments.

It is a type of fraud that predates the Internet. All an identity thief needs is a stolen wallet or purse. Other methods of obtaining personal data include stealing mail and searching through garbage. But the Internet extends the criminal's reach, allow-

ing him or her to steal identities without physical contact or geographic proximity. Privacy advocates and credit agencies estimate that more than 500,000 people will fall victim to identity theft this year. Most experts attribute the growing toll to the Internet.

Empty bank accounts

The scope of the fraud can extend from long-distance calls or credit card purchases to emptying a victim's bank account or taking out loans in the victim's name. Even worse than credit-related identity theft is criminal identity theft—when someone commits crimes using the identity of someone else and gives that person a criminal record. The victim usually knows nothing until bills come in or a routine traffic stop turns into an arrest. A victim of identity theft is usually not liable but spends time and aggravation trying to sort out the damage and restore credit ratings and a good name. A privacy rights group estimates that the average victim will spend two years trying to get \$18,000 in fraudulent charges straightened out. Businesses have to absorb the loss, affecting the cost of goods and services.

The impersonal aspect of electronic transactions benefits criminals, according to the National Fraud Center. If a thief with a stolen credit card tries to buy something in person, he or she faces physical limitations. The thief must be present for the transaction, risking detection and arrest. He or she must sign the receipt, allowing comparison with the signature on back of the card. None of these deterrents apply in the anonymous electronic world.

Congress tackles the problem

Congress is moving forward on several fronts to combat Internet-aided identity theft. The Senate Appropriations Committee is offering a bill that would prohibit "displaying to the public" a Social Security number without consent, but that bill exempts Internet research services. In the House,

(continued on next page)

Internet-aided identity thieves on prowl

Computers allow access to personal data, cloak criminals in anonymity

(continued from preceding page)

a tougher bill would outlaw the sale of a Social Security number and also prohibit the withholding of services from a customer who declines to give a Social Security number to a vendor. Current law allows states to sell drivers' records with Social Security numbers; the House bill would prohibit that.

The Senate Government Affairs Committee's Subcommittee on Investigations conducted a hearing on identity theft in May 2000. The subcommittee's chief investigator thinks businesses should be alert to the problem. "Every company needs to look at its internal policies," he said. "The hearing points up the need for background checks on potential employees or even vendors." With the Internet, he said, someone can hand you a fake driver's license or Social Security card. "With Web sites selling phony certificates," the investigator warned, "someone could show you a Red Cross certificate or a computer certificate or a teaching certificate—and they could be counterfeits."

The Subcommittee on Investigations focused on three kinds of fake-ID enterprises:

1. Some Web sites sell high-quality documents in the customer's name. Thus, the purchaser can augment his or her accomplishments with phony certificates.
2. Web sites sell high-quality computer templates so a buyer can make his or her own phony documents.
3. Some criminals do it themselves. A 23-year-old convicted felon testified at the hearing that he used the Securities and Exchange Commission Web site to get the Social Security numbers of people listed in company filings. He then created a birth certificate, a driver's license and a W-2 form in the other person's name. He got car loans on the Internet using the stolen identity and purchased a \$40,000 car.

Web sites sell fake IDs

The Subcommittee on Investigations staff investigated 15 Web sites that either sold fake documents or offered templates. Staffers obtained a counterfeit driver's license, templates to produce fake licenses, authentic-looking birth certificates and documents to fabricate credentials for employment. One Web site advertised a fake ID kit with "college transcripts you customize, college diplomas, new birth certificates, green cards, Social Security cards, driver's licenses and more." The site proclaimed: "We provide you with templates and step-by-step instructions on what you need to create fake IDs so real you could fool your own mother."

The chief counsel of the subcommittee said in testimony, "The Internet offers many exciting opportunities for commerce but, as our investigation has shown, it can offer inventive criminals more effective tools to engage in illegal conduct."

Although the sites offer disclaimers about the documents being for novelty use only, the marketing strategy promises credentials that can get you a job. "Receive access to authentic downloadable certification certificates to get you a job as an Activity Coordinator," one site promises.

As required by federal law, some documents come with the words NOT A GOVERNMENT DOCUMENT printed in red ink on the lamination, but the disclaimer can easily be removed by trimming off the top of the lamination and removing the document.

"The Internet has greatly facilitated the manufacture and sale of counterfeit identification documents by allowing sellers to mass-market high-quality fake IDs with virtual anonymity," the subcommittee's chief counsel testified. "The distribution of these counterfeit materials is growing because of the expanding technology of the Internet. It will be no easy task to maintain the integrity of the identification documents on which both the government and the private sector rely."

Higher quality, lower prices

A fraud investigator for the Florida Alcoholic Beverages and Tobacco Division testified at the subcommittee hearing that the Internet represents the largest opportunity to produce, market and sell high-quality false identification.

He estimated that 30 percent of false IDs now come from the Internet. Computer technology allows the creation of the basic template needed to produce the fake document and allows transfer of that template via e-mail or downloads. Falling prices for powerful computers and high-quality printers allow individuals to use templates from the Internet to make their own fake IDs. Web sites offer instruction on making a hologram or laminating a fake ID.

The Florida investigator pointed out that counterfeit identification available over the Internet duplicates many features of legitimate identification. For instance, counterfeiters on the Internet are copying security features like holograms, microprinting and bar codes. Such sophistication makes it harder for a business to distinguish the fake from the genuine.

Web sites offer to sell identification documents for all 50 states. "High-quality identification cards can be purchased by anyone, in any name, with any date of birth, for prices ranging from \$30 to \$300," he testified. Some false ID sites have gotten over 10,000 hits in a single day. One Web site he investigated used sales representatives on college campuses. After a search warrant and arrest, the suspect said he had made \$1 million from sale of fake IDs.

Examples of identity theft are often in the news:

- In September 2000, a fake diploma and transcript from the University of South Florida were offered for \$50 on a popular online auction site.
- Last spring, undercover agents from the GAO posed as plainclothes officers and penetrated

security at 19 government offices. They used credentials made with computer programs and badges purchased over the Internet.

- In 1998, a man presented a fake FBI badge to a motel clerk in Kentucky and gained entry to a room, where he waited to rob and kill the occupant.
- Earlier this year, an electronic thief stole consumer data from an Internet seller of compact discs, including up to 300,000 credit card numbers. A computer scientist with a technology services company predicted that if database vulnerability persists, credit card companies will no longer absorb losses.
- In one federal prosecution, the defendants obtained the names and Social Security numbers of U.S. military officers from a Web site, then used 100 of those names and numbers to apply for loans via the Internet at a Delaware bank.
- In another federal case, the defendant obtained personal data from a federal agency's Web site and then used the data to submit 14 loan applications online to a Florida bank.

What can businesses do?

As Congress works to protect privacy and curb the sale of fake documents, what can businesses do? Companies can be both the victims and the unwitting accomplices of identity thieves. A job applicant can supply phony credentials, and companies risk liability if lax controls allow criminals physical or electronic access to their customers. In many cases, businesses must absorb the loss in fraudulent transactions. The Privacy Rights Clearinghouse, a nonprofit advocacy group, offers these guidelines:

Privacy policy: Businesses should develop a comprehensive privacy policy that includes responsible information-handling practices, such as proper document disposal (shredding or incin-

(continued on next page)

Internet-aided identity thieves on prowl

Computers allow access to personal data, cloak criminals in anonymity

(continued from preceding page)

eration). Limit the amount of information collected from customers. For instance, is the Social Security number really necessary? Avoid printing employees' or customers' Social Security numbers indiscriminately on paychecks, parking permits, badges, mailing labels and the like. Educate employees about handling sensitive data.

Computer security: *The Lipman Report* has devoted several recent issues to electronic security, including September's report on information technology threats of the future. Companies should limit access to personal data on customers or staff to those employees with a legitimate need. Physical access to critical hardware should be restricted. Password protection may not be enough to safeguard sensitive data. Personal information should be encrypted for electronic transmission.

Background checks: Companies should verify that applicants or vendors are who they say they are and that their claims are true. An applicant may be obscuring a poor driving record with a phony license or claiming expertise with fake credentials. Pre-employment screening should verify work history, education, personal and employment references, and the absence of a criminal record. A company might face liability if a victim of identity theft traces the crime to an employee with a criminal past.

Credit crackdown: Credit issuers should do better at identity verification. They should improve identity-checking procedures for "instant" credit, favored by identity thieves. Photographs on credit cards would cut down on fraud, as would adopting smart cards, which store information in microprocessors.

Authentication: The process of verifying someone's electronic identity becomes critical as the pace of e-commerce increases. As we reported last month, digital signatures offer greater protection for Internet buyers and sellers.

Companies focused on security will be positioned to handle electronic security demands. If security is part of the corporate culture, if employees are educated about security needs, if management sends the signal that security is important, then the extra steps necessary to deter identity theft will not be a burden. Electronic security becomes a fact of corporate life.

Companies can support governmental action. Congress has reached a consensus that curbs are needed on the dissemination of Social Security numbers. Other roadblocks to criminals are being considered, such as tightening controls on the sale of fake documents over the Internet

This year, Electronic Frontier, a report to the President of the United States, put the problem this way: "The Internet provides unparalleled opportunities for socially beneficial endeavors—such as education, research, commerce, entertainment, and discourse on public affairs—in ways that we may not now even be able to imagine. By the same token, however, individuals who wish to use a computer as a tool to facilitate unlawful activity may find that the Internet provides a vast, inexpensive and potentially anonymous way to commit unlawful acts, such as fraud."

Innovative, forward-looking companies will eagerly seize opportunities on the Internet. Those same companies will be proactive in adopting electronic security measures. As criminals seek to exploit the speed and anonymity of the Internet, businesses can fight back by controlling access to data and demanding verification of identity.

As we move into the new electronic frontier, we must seize the latest advances in security services and technology to make Internet business safe or risk losing customer confidence.



The Lipman Report Editors