**Keep your CU ahead of phishers and other ID theft criminals.**

# *ID Theft Tools Nip Fraud*

PATRICK TOTTY

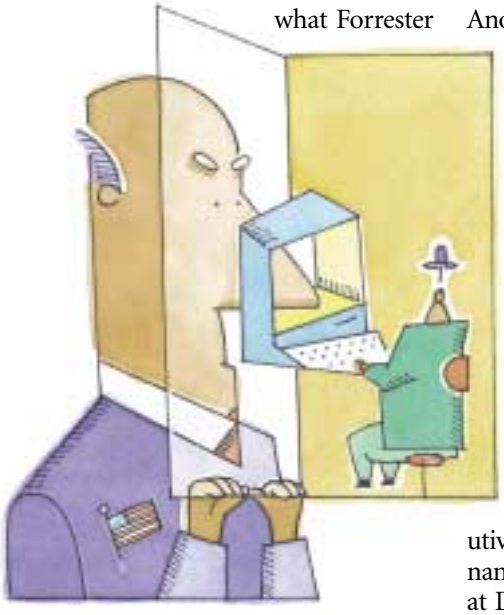
KEVIN FORRESTER knows a Federal Trade Commission statistic that will make even the most jaded jump up and take notice: "Identity theft in the past five years has affected 27 million Americans—one-tenth of the U.S. population."

Forrester is group vice president of identity (ID) theft services at Liberty Enterprises, Mounds View, Minn. Liberty offers anti-ID theft services supplied by Identity Theft 911 in San Francisco.

"The most common form of ID theft is account takeover, where a thief takes your credit card information and goes on a spree," he says. "The spree usually is over within 24 to 48 hours, and its effects are fairly easy to resolve."

But then there's what Forrester calls "true ID theft," in which criminals strip-mine almost every essential financial datum a person has: name, Social Security number, personal identification numbers (PINs), and bank and credit card account numbers. "They try to open up additional lines of credit using your information," Forrester adds. "It's the form of ID theft people fear the most."

Forrester says ID thieves commit the crime because it's easy to do so—and not in the sense of using some sophisticated software. "Most of the information criminals need comes from dumpster diving for hard-copy records or getting information stolen from a business."



## Something phishy

Another rich source of information for ID thieves: phishing. Phishers hijack elements of a financial institution's Web site, such as the logo and look. Then they send out e-mails asking recipients to contact the institution and verify or update vital information such as account numbers and PINs.

"Ironically," says Dennis Maicon, executive vice president of financial services solutions at Digital Envoy in Atlanta, "70% of phishing is from outside the U.S. International crooks, based in places like Russia and Malaysia, sell phished information to U.S. criminals." (Digital Envoy produces IP Inspector™ Fraud Analyst ID verification software.) One of the biggest giveaways that an urgent e-mail from a financial institution is a phishing device is its ungrammatical English.

"Generally speaking, banks are more likely to be targets of phishing than credit unions because they generally have larger customer bases," says Roger Nettie, solution development manager and a risk management specialist at CUNA Mutual Group in Madison, Wis. "However, we recently ran into a case where a university credit union had its computer used to phish the university community."

Despite credit unions' current under-the-radar status with phishers, they still have problems with ID theft, says Nettie. They often can't tell whether a fraud fits the ID theft category. "What determines ID theft? Does a claim always fit that category? There's often no way to say yes or no." The categories include forgery, electronic crime, fraudulent deposits, and credit card transactions.

Maicon agrees financial institutions don't always know how to distinguish between conventional fraud and ID theft. But, as many credit unions track the origins of fraud, namely tracing a fraud back to the intentional opening of bogus accounts opened with stolen IDs, they're getting a better statistical handle on things.

## New technologies

ID thieves operate under the assumption that their fraudulent activities don't have any antidotes. "A crook in Atlanta goes online with a stolen ID and tries to open a San Francisco credit union account," says Maicon. "The credit union sees normal account activity until bam!—the account is cleaned out. The usual credit checks didn't detect the scam."

But with software like IP Inspector Fraud Analyst, the Atlanta scammer could be flagged and put under suspicion for a host of reasons. "The tool looks at an IP [Internet protocol] address and asks questions such as, 'is it an anonymous proxy?' If it is anonymous, nine times out of 10 you won't want to deal with it," Maicon says.

Time of day is another possible indicator, he adds. "If an online application comes in at 3 a.m., it looks suspicious." Other factors include geographic location—why enter a Califor-

nia address if the financial institution is in Georgia?—and whether the person is using a free e-mail account.

Also, does the request come from a domain in a country where known fraud artists congregate?

Even criminals who have successfully stolen IDs must face a battery of authentication checks, says Maicon. One is a log-in verification module. "Typically, 80% of online banking traffic comes from a member's home or workplace in the same city using the same Internet service provider. Based on that pattern, we can develop a reliable user profile. If the user suddenly logs on at an odd time of day or at an odd location, the authentication system notes the behavioral inconsistency and can throw out an additional authentication checkpoint, such as asking questions to see if this is the real person." A question might include, "What are the major crossroads near you?"

Maicon says traditional fraud detection systems, such as credit bureaus, Social Security number checks, and address verification systems yield a 40% detection rate. "We're catching 60% to 70% more than traditional systems. A lot comes from crime rings that try to open accounts all over with the same IDs or mailing addresses."

One scammer in California tried to open 20 or 30 accounts a day in locations ranging from South Dakota to Atlanta. "Many scammers are like workaday folks: They sit down at their PCs and methodically do their business," Maicon says.

### The educational angle

Anti-ID theft services often have an educational component. Forrester says Identify Theft 911 will aggregate information from the Federal Bureau of Investigation, Secret Service, and U.S. Postal Service and then e-mail alerts to members. But beyond educating members, credit unions also should dispel needless fears.

"Many people fear someone will steal their ID while they're doing a transaction online," Maicon says. That can't happen: Modern computer encryption is too secure. But members should be told that. "Having anti-ID theft tools reassures members that their credit unions are taking precautions."

Nettie says members can get stung online but not from ID theft. "A common scam for online sales is when you're selling a car and you receive a cashier's check from a buyer for more than the amount you asked for. The person who sent you the check asks you to reimburse the overage. You comply, later finding out the check was a phony and the scammer pocketed the difference."

Credit unions also can assist with resolution, when an ID theft victim begins the task of restoring credit. Through Identity Theft 911, staff belonging to the International Association of Financial Crimes Investigators, El Dorado Hills, Calif., can assist ID theft victims. Credit unions can sign up for the service and cover members, refer members to the service, or invite them to independently sign up for coverage.

Four states now have laws permitting ID theft victims to place a "security freeze" on all their accounts. The freeze prevents the opening of any new accounts in the victim's name unless the victim specifically deactivates the freeze using a special PIN.

"It's almost an arms race," says Maicon. "Criminals always look for new ways to circumvent safeguards. But their opponents are very smart and dedicated."

*For more information, visit* CreditUnionMagazine.com