High-tech tools help members, CUs thwart the rising tide of this pervasive crime.

Hard Times Boost Identity Theft

PATRICK TOTTY

"APPROXIMATELY one-third of all identity theft is credit-related, and incidents of identity theft are up 22% since 2007," says Steve Schwartz, executive vice president of consumer solutions for Intersections Inc.

Based in Chantilly, Va., Intersections is a Credit Union National Association strategic alliance provider. "As unemployment increases," he says, "crime rises—especially identity theft."

"Identity theft is the No. 1 consumer complaint reported over the past five years to the Federal Trade Commission," says Tom Oscherwitz, chief privacy officer and vice president of government affairs at San Diego-based ID Analytics Inc.

Both men are members of the identity theft protection industry that—thanks to hard times, government requirements, and the eternal curse of fraud—credit unions should ally themselves with closely.

Types of identity theft are changing. "Traditional identity theft has plateaued," says Steve Reger, director of TransUnion's fraud victims' assistance department in Fullerton, Calif. "Crooks are looking at other fraudulent activities. With the current economy, we're seeing an increase in average Joes fraudulently using Social Security numbers, such as their children's, or filing fraudulent credit repair reports either to get new credit or to get out of paying debts."

People file false reports and then ask for copies, which they send to creditors as "proof" they can't pay, Reger explains.

Medical identity theft also is burgeoning, says Matt Cullina, CEO of Scottsdale, Ariz.-based Identity Theft 911. "It's probably the most complex type of identity theft to resolve because there's no central data organization to clear the fraudulent activity, and [Health Insurance Portability and Accountability] laws are so stringent. We have to connect with every provider or entity the fraudster interacted with while getting medical assistance to resolve the situation."

People who steal medical identities use them to gain emergency room visits and access others' medical insurance without charge. "Worse is that a victim's height, weight, blood type, allergies, and other medical information are highly unlikely to match the fraudster's, so untangling a stolen medical identity also means purging misinformation."

Another trend is "synthetic" identity fraud, Oscherwitz says, where fraudsters combine real and fabricated identity elements to create a new identity, then use the new synthetic identity to build a real credit file. "One technique is Social Security number 'tumbling,' where fraudsters change one or two digits in a real Social Security number to create fake numbers that escape detection because they match numbers typically associated with a particular year and birthplace."

Protective measures

Arrayed against iden-

Advance Scoring Predicts Risk

ID Analytics Inc., San Diego, offers a three-digit identity score called ID Score®. The higher the score, the more likely the person being scored isn't who he or she purports to be. The score is based on cross-indexing identity elements from many sources, including retailers, financial institutions, and telecommunications.

"A suspicious score creates an 'identity risk event,' something that assumes greater importance under the USA PATRIOT Act's requirement that financial institutions know who their customers are," says Tom Oscherwitz, ID Analytics' chief privacy officer and vice president of government affairs.

Information going into a score includes:

▶**Basic identity elements,** such as name, address, and phone numbers. "We look for anomalies, such as five people using the same Social Security number, two applicants on the same day from the same address, or a history of fraud."

▶**Electronic identity elements,** such as e-mail addresses.

"When we provide a score to a credit union, we provide 'reason codes' explaining why we've given a person a certain identity score," says Oscherwitz. "For example, an unusual number of applications for credit in a short time may appear suspicious. On the other hand, we might indicate we found no unusual activity—a good reason for a low score.

Identity scores help credit unions focus resources on the pool of applicants most likely to pose identity fraud risks, he adds. "A high identity score, for example, will trigger additional steps to verify an identity, such as manual review or asking the applicant to provide more documentation."

tity thieves are tools enabling credit union members to detect, repair, and even prevent identity theft. For example, TransUnion provides monitoring tools, usually linked through credit union Web sites. They allow members to monitor all three credit bureaus or just TransUnion. Costs are monthly, depending on the level of monitoring and frequency of use.

TransUnion also notifies members of changes. "For example, we'll send an e-mail anytime there's a query from a creditor which, if you haven't applied for new credit, indicates somebody may be attempting identity theft," says Linda Vance, vice president of credit unions at TransUnion's Financial Services Group.

Vance says users can freeze or lock their credit files in all 50 states. Members get a code that gives them access to freeze or unfreeze their credit files. A freeze slows down the automated decisioning process so would-be lenders can't just pull a credit report but must directly ask the consumer for it.

But if members already are identity theft victims, TransUnion will add alerts to their credit reports, Reger says. Typically, when identity theft occurs, vendors:

▶ **Assign** a case number and case manager;

▶ **Help** members contact and file affidavits with financial institutions, utilities, governments, and other authorities; and

▶ **Close** avenues, such as credit card accounts, or freeze credit if necessary.

In addition to its own suite of branded products, through its exclusive partnership with the Identity Theft Assistance Corp. (ITAC), Intersections has developed a full suite of products, ITAC Sentinel®, to help consumers protect themselves from identity theft.

"Customers receive their credit report with data from either one or all three credit agencies—depending on which service they choose—with updates, monitoring services for both credit and public data, and exclusive access to ITAC's restoration service," Schwartz says.

"Credit monitoring is a necessary fraud detection tool, but it's reactive, detecting something that may have already happened before detection. We help members cover the broadest spectrum possible by monitoring public record data including utilities, cell phones, criminal records—data that may never otherwise appear on a credit report but that's accessed easily by criminals."

The service also monitors:

▶ **Thousands of databases** for unauthorized change-of-address notices, utilities in members' names, and more;

▶ **Duplicate use** of Social Security numbers; and

▶ **Credit and bank account** numbers in unsecured areas of the Internet.

It also provides password protection, anti-keylogging software, and mobile transaction protection.

Guarding life stages

Vendors tailor offerings to fit members' life stages, Cullina says. "One stage assists parents and their children. Children are a fast-growing segment of identity theft because people often steal their Social Security numbers, knowing it will be several years before fraudulent use is detected. We connect to TransUnion to see if a child's Social Security number is being fraudulently used. If so, we can lock down the child's credit file until he or she turns 18 and try to resolve the fraudulent activity.

"Another stage focuses on the other end of life's spectrum," Cullina adds. "Identity thieves often target obituary pages, stealing identities to open new credit accounts before probate. Our program works with surviving spouses to lock down the deceased's credit file right away."

Sometimes people think they have to wait for a problem to emerge before using an anti-identity theft service. "We encourage people to call at the earliest sign of a problem," Cullina says. "About 55% of cases are proactive in nature—a member receives something suspicious in the mail and has questions. We investigate and often help stop theft before it gets underway. The remainder of our cases are post-fraud, where we help resolve cases by securing affidavits and police reports, and notifying creditors and credit bureaus."

He says the credit union movement has been receptive to expert identity management service vendors because of their focus on member loyalty versus fee generation. Credit unions "understand this is an excellent value-added service to offer members, who see it as a sign the credit union cares about them."

For more fraud prevention information, visit CREDITUNION magazine.com

Resources

▶ CUNA strategic alliance provider: Intersections Inc., Chantilly, Va.: 703-488-6100 or *intersections.com.*

▶ ID Analytics Inc., San Diego: 858-312-6200 or *idanalytics.com.*

▶ Identity Theft 911, Scottsdale, Ariz.: 480-355-8500 or *identitytheft911.com.*

▶ TransUnion, Chicago: 866-922-2100 or *transunion.com.*