

To Stop a Thief

With identity theft rising, companies need security that turns off fraud—but not customers.

IDENTITY THEFT MAY be a quiet sort of crime—no bullets, no gore—but it certainly leaves its mark. Using fraudulently acquired information like Social Security numbers, financial data, or website passwords, thieves pass themselves off as people they're not, buying goods, opening credit card accounts, and transferring bank balances. The victim's credit rating takes a beating, and fixing it can be a difficult process—one that an increasing number of Americans are dealing with. According to a 2010 study by Javelin Strategy & Research, 11.1 million Americans were victims of identity theft in 2009, a 12% increase over the previous year.

But it's not just consumers that are harmed by identity crimes. Companies that are duped by identity thieves can lose customers and business. Indeed, according to the "LexisNexis 2010 True Cost of Retail Fraud Study," one in three consumers who were victims of fraud will avoid certain merchants, and one in four will spend less money. There can be legal consequences, too. The federal Red Flags Rules, created under the Fair and Accurate Credit Transactions Act of 2003, require a broad range of businesses, including financial institutions and many retailers, to implement systems to detect behavior

that could signal identity crime.

Of course, businesses could slam the door on much identity theft by increasing security and requiring an array of passwords and challenge questions (e.g., "What was your mother's maiden name?") for every transaction. The problem with this approach, however, is that it can make for a burdensome user experience. "You can eliminate risk by making the process very difficult, but that will alienate your customers," says Dennis Becker, vice president at LexisNexis.

The better approach, says Becker, is to consider each customer and each transaction individually and ratchet security up or down as needed. So instead of treating all customer inquiries as having the same level of risk—and always employing the same layers of security—build a nuanced picture of what is happening in each case, and tailor security to that. You would then treat a customer who regularly performs balance transfers from the same computer differently than a customer who requests a transfer from a device the bank's servers have never interacted with. "You want to put in the higher controls when you need to, while avoiding friction with your customers," says Becker.

LexisNexis leverages an array of technologies to strike a balance in managing identities. Sophisticated analytics let companies home in on outside-the-norm behavior, so that they know

when to turn up the defenses. Also crucial are real-time access to vast repositories of data—billions of public records stored in tens of thousands of databases—and the ability to link relevant pieces together.

"Effective linking lets you do a lot of the verification behind the scenes," says Becker. "So you'll have more confidence that the person asking a utility company for a senior discount is the right age and really does live at the address given."

The idea is to verify your customers' identity without inconveniencing them. Done right, identity management can build relationships and drive revenue. It shouldn't be disruptive—except, of course, to the identity thief. ●

—Alan Cohen

YOU NEED TO STRIKE THE RIGHT BALANCE IN IDENTITY VERIFICATION TO AVOID FRICTION WITH CLIENTS.

12.5%

RISE IN IDENTITY THEFT FRAUD IN THE U.S. IN 2009, TOTALING \$54 BILLION.

Source: Javelin Strategy & Research

Now You Know.

Identity Management makes it possible to see the forest *and* the trees.

Quickly navigate the landscape of identity management. Ask for the right information from *each* customer to increase transactions and establish trust with them *all*.

Shift your focus and find out what you need to know. Now.

View webinars at idmanagement.lexisnexis.com

 LexisNexis®