ABA Banking JOURNAL

Tech topics

Will you spend to thwart ID theft?

Internet based or not, ill-protected records are yielding criminals a license to steal. Vendors and bankers want to fight back

When it comes to identity fraud and its narrower cousin, identity theft, the Federal Trade Commission is on red alert and banks are rethinking the issue of combating thieves who lift legitimate account holder's credentials to line their own pockets.

You could say the tipping point occurred with headlines from February's ChoicePoint data breach and the Alpharetta, Ga.-based firm's required disclosure under California law.

Or, that the issue was greenlighted to greater importance soon after with an insider infiltration of a database at a newly acquired subsidiary of New York City headquartered LexisNexis, itself active in the ID theft prevention market. (Although no known cases of identity theft have, as of yet, resulted from these events, there is a high correlation between breaches and subsequent spikes in consumer accounts fraud.)

Clearly, there has been a spike in consumer awareness and anxiety. It has helped to generate renewed industry interest in a chronic problem. In terms of

By Lauren Bielski, senior editor

what the hard evidence illustrates, reported complaints of ID theft have shot up to 9.3 million from 500,000 in 2001, according to the FTC and other sources.

Before recent events and headlines, leading banks were already struggling to work more effectively with law enforcement and considering which channels to monitor. Certain ATMs, as an example, can be altered to take in account and password information and new account fraud tends to occur in the branch. Moreover, the most progressive banks have taken steps to address problems particular to their organizations.

But ID theft continues to confound more than a few financial services firms with its shifty form. Some variants include new account opening with a false identity and account takeover—or use of stolen information to say, pay the bills of the thief, who is perhaps more desperate than professional in that instance.

To this day, the topic inspires mixed industry commentary, particularly "on background," where an astute listener will notice that all the experts have a distinct opinion about (1) whether the problem really is significant enough to take "drastic action" against it; (2) what root causes of ID theft are the "best ones" to address; and 3. whether the problem will spike further or gradually level off and become a non-issue on its own over time.

If short-run patterns are any indication, ID fraud will only continue—gushing before it settles into a trickle.

Yet all sources seem to agree on this point on and off the record: as part of an operational risk management plan, banks need to have some strategy in place because of the potential impact of ID theft on their brand and because it can erode consumer confidence in the banking industry.

Synergistic effect

Today some of the terms of debate have shifted, but talk, and, finally, action, has intensified in an effort to head criminals off at the pass.

Consider phishing attacks, which have reared their collective ugly head over the last two years. These have also promoted interest in addressing ID theft and fraud, as the technique represents yet another way to harvest account information.

In this variation, phishers trick unwitting internet users into giving up account information by presenting legitimate looking e-mails that link to phony web pages, which harvest data.

Some technologists believe that—as phishing "automated" the information gathering that can lead to other types of fraud—capabilities such as scripts, Trojans, "bots," and spyware will be increasingly used to set other aspects of fraud spinning out in a no-holds-barred auto-attack.

"It's conceivable that fraud will have a mechanized aspect in the future," says Eli Katz, practice director in the global financial services practices, Unisys, Blue Bell, Pa."If that happens, phishing will only be part of a broader, automated theft industry," he explains, adding, "Certainly today, there is more to the story of ID theft than phishing."

And when it comes to identity theft and broader frauds, synergy—as well as technology—can help the criminally minded just as well as any strategist. With it, the internet, phone, and branch offer complementary fraud gateways with dumpster diving, check stealing and fabrication, false driver's license creation, and host of other crimes and methods coexisting in a parallel universe of harm.

"The big message lately is that identity theft isn't going away and that it is expressing itself as a multi-channel problem in need of a full breadth solution at banks in retail environments," says David Helsper, vice-president of engineering and product development for Digital Envoy, Norcross, Ga.

Although Digital Envoy sits firmly in the anti-phishing, online protection arena, Helsper knows that sophisticated banks have begun thinking more broadly about data protection; how marketing is handled; and what account information is allowed to flow freely in the mails, for instance.

"Unfortunately, there's no silver bullet solution for identity theft," agrees David Dorn, vice-president of new business development for Deluxe Financial Services, St. Paul, Minn.

"This is why bankers need to evaluate an array of solutions and develop a program that addresses many aspects of ID theft both online, on the telephone, in the branch, and at the ATMs."

For instance, the company is providing a service called IDTheft Block, which monitors and flags irregular account activity to consumers.

Multi channel, multi method problem

Other sources agreed that what ID theft calls for is multi-pronged treatment, with a re-examination of account opening processes, for example, on equal footing with tight security and the use of overall data protection strategies.

Banks will need to do a fairly complicated risk analysis to determine what makes sense for them in terms of response.

"There are always decisions to be made about the level of risk tolerance that is acceptable, say, with doing online mortgage origination versus what is the acceptable amount to spend on automation [to help curb fraud]," says Ted Crooks, vice-president of global fraud solutions for Fair Isaac, San Rafael, Calif, which offers many anti-fraud solutions.

Crooks indicated—and he was not alone—that there is a new interest in applications that can flag irregular account activity or help to establish that someone presenting credentials holds them legitimately.

Technology may be ultimately useful because it lets banks sift through and find the exceptions and potential problems in real time.

"ID theft should really be responded to as a bank robbery would be," says Joseph Ansanelli, chairman and CEO with Vontu, San Francisco.

Ansanelli has testified before Congress about the importance of data protection and other broad business process controls that have the net effect of creating a more controlled business environment.

If a bank has the right controls and applications in place, they have greater visibility into fraud closer to the time it happens.

"As with a direct theft of cash in a physical location, ID theft requires protection, detection, and correction. Some institutions need to improve how they help consumers through this. Crooks of Fair Isaac made many of the same points. He also added, "some banks need to have a better sense of the net effect of ID theft on their operations."

Chief in the call for a multi-channel,

multi-pronged response is Javelin Strategy & Research, Pleasanton, Calif. Principal James Van Dyke did research on 40 banks and presented his findings about common business practices—information exposures of paper and electronic documents that led to insider theft or common marketing practices, for instance—at a recent trade show. "The patterns of attack differ, so banks need to rethink business processes and set themselves up to register a variety of problems, such as considering what they send through the mail in the first place," Van Dyke said.

Phantom numbers; bigger problems

Despite the increasingly high profile nature of ID theft and problems like phishing that have erupted since, many banks remain in "wait and see" mode rather than actively reviewing solutions, purchasing and installing them, say many sources on background.

One reason for this may be the lack of reliable national identity fraud stats that give true scope to these crimes. There are only guesstimates, notes Dr. Gary Gordon, professor of economic crime programs, and executive director of the Economic Crime Institute at Utica College. "Many figures I see quoted in the press are way, way off," Gordon says.

As a result, bankers get skeptical. "So you have individuals on one end of the spectrum doubting that the problem is big enough to require a big guns response," Gordon explains. "Others may think that [fraud] is such a chronic and shifting problem that a given company couldn't possibly afford to implement any sort of truly effective authentication or response solution."

Still, Gordon thinks a stepped up response—particularly on authentication—is required. First, consumers who are hit up are hit hard, and it takes time, effort, and aggravation to get credit ratings back on track. Moreover, bankers need to respond because of ID fraud's potential role in funding terrorist organizations or complicated fraud schemes that can put the economy at risk.

"[Terrorists and criminals] are using our complicated financial system against us," says Republican congressman John Carter of Texas. "We have to get on this." "This," for Carter being border control, use of more secure identification, and new collaboration between the financial service industry and law enforcement that makes fraudsters easier to catch.

Carter authored the recently enacted ID Theft Enhancement Act that provides stiffer penalties for thieves that have engaged in identity theft in their overall crime. "Make the punishment stiffer and you'll motivate law enforcement to do the hard work that white collar criminal prosecution requires," Carter says.

Gordon also advocates stiffer penalties as well as the use of national identity cards or more secure state issued licenses, given the high costs and complications of developing the former.

"Banks," he points out, "depend on the driver's license to establish a working relationship with an account holder." To address synthetic identity problems, Gordon also proposes more complex authentication tied to account opening.

"Biometrics and certificates, which might work well in the business to business sphere have not been accepted in the consumer sphere," he explains.

In his work with Lexis/Nexis to formulate the solution now on the market, called InstantID, he's come to consider different approaches. "It makes sense to use information-based authentication, where data on a form will be checked in real time against external databases to make sure all data points 'fit' and belong to the applicant," Gordon says.

Eli Katz of Unisys also has several suggestions.

"Banks need to revamp their current archaic systems with tools that take advantage of the same technology that cyber-thieves use," he notes.

"For instance, institutions need to go beyond reliance of simple PIN or password protected web transactions by implementing monitoring, encryption, and other bank-initiated safeguards."

But it's not all about technology. As with operational risk management itself people and processes play a role. Katz and others suggest banks develop strong, institution-wide policies on identity and access management. This would go beyond who can access and control customer data in a given instance but would include how these users are authenticated and monitored in their work. The objective is to create what Unisys calls a trusted enterprise.

Banks might also consider creating and implementing a special department dedicated to monitoring potential fraudulent activity across the entire bank.

This group would be provided with real-time fraud detection data that could be shared across the organization, not be trapped in isolated data warehouses. ***BJ***

Resources to address ID theft

Business Info. Group
employee screening
www.bigreport.com

Deluxe Financial Services
IDTheftBlock
www.Deluxe.com

Fair Isaac
Falcon Fraud Manager
www.Fairisaac.com

IDAnalytics
multiple solutions
www.idanalytics.com

LexisNexis
InstantID
www.LexisNexis.com

Nuance
biometrics; VoicePrint
www.Nuance.com

Primary Payment Systems, Inc.
Identity CHEK
www.Primarypayments.com

Qsent
iq411
www.Qsent.com

Symantec
Online Fraud Management
www.Symantec.com

Unisys Corp.
risk management services
www.Unisys.com

Vontu
anti-phishing vendor
www.Vontu.com

Vocent (partners with Intervoice)
biometrics
www.Vocent.com

Reprinted from April 2005 ABA Banking Journal © by the American Bankers Association.
For more information about reprints from ABA Banking Journal, contact PARS International Corp. at 212-221-9595.