



# IDENTITY CRISIS

*Online banking struggles to balance multifactor authentication security with customer usability*

BY CARLI FLIPPEN

**T**hree years ago, the First American National Bank in Luka, Miss., was in the same position as most community banks.

Like many other banks, First American National offered Internet banking via third party vendors featuring basic user ID and password security that fraudsters and other thieves were quickly learning to circumvent.

Then the Federal Financial Institutions Examination Council (FFIEC), looking to reduce data breaches, released a set of new guidelines that directed all financial institutions to beef up user authentication security for their electronic banking services.



## IDENTITY CRISIS

Two years later, in response to the FFIEC multifactor authentication guidance, the \$220 million-asset bank has added additional online authentication security measures. Through the combination of machine analysis and mutual identification, consumers are verified (via knowledge questions and computer identification analysis) before gaining access to sensitive information as contained on bill payments and e-statements.

About 90 percent of financial institutions are estimated to be in compliance with the guidance, according to the research firm Celent LLC.

First American National Bank's response to comply with the FFIEC guidance is typical of the

iar computer, the security tool requires them to answer a series of challenge questions before granting them access to the online services. Customers, of course, provide the answers to the questions when they originally register at the site.

First American National requires its customers to answer a series of questions to verify their identity online. The bank uses both mutual authentication techniques, in the form of challenge questions, and machine analysis. In the latter, the customer may register his computer with the bank, which then places an electronic tag or "cookie" on the customer's computer. When the customer returns to the site, the bank's Internet banking system

**“You can use all the technology and fancy tools you want ... [but the best security] is transparent and relies on the good sense of the folks using it.” – JACOB JAEGER, TECHNOLOGY CONSULTANT**

additional authentication security measures that have been adopted by financial institutions nationwide. Most community banks are adopting a combination of mutual authentication and machine analysis tools,

says Celent analyst Jacob Jaeger.

For mutual authentication, a bank asks customers to select a set of icons—pictures or phrases that the bank will present to them each time they sign in to access online services. If the customer doesn't recognize the personalized combination of images and phrases, the bank does not allow him to log in.

Machine analysis tools capture the unique identity of the computer that customers typically use to log in. If customers try to log in from an unfamiliar

computer, the security tool requires them to answer a series of challenge questions before granting them access to the online services.

Other authentication technologies on the market include equipping customers with token-based systems and providing one-time passwords via a customer's mobile devices. While offering excellent security, most community banks found such systems unreasonably complex for the typical retail customer or prohibitively expensive to deploy widely. Such authentication measures are more appropriate for cash management and corporate banking environments, Jaeger suggests. Tokens and one-time passwords are too expensive and cumbersome for retail operations. However, corporate users who are more sophisticated and have more assets to protect may be more open to the burdens of using those systems, he explains.

First American National outsources its electronic banking services to two third-party providers—Metavante and Ipay Technologies. The bank asked those two companies to propose multifactor solutions, and both came back with security-question tools. “That seemed to us to be the most feasible solution,” says Greg Windham, information security officer for the bank. “We couldn't afford to mail out tokens and still offer free Internet banking.”

The vendors implemented the security technology quickly and smoothly, taking the

### Meeting Mandates

In October 2005, the Federal Financial Institutions Examination Council (FFIEC) issued guidelines that directed banks to assess their security needs and deploy multiple levels of identity protection beyond user name-and-password screens to their electronic banking operations.

The FFIEC gave banks until January 2007 to assess their vulnerabilities and institute some multifactor authentication or layered security procedures. Although the FFIEC did not prescribe sanctions for noncompliance, the 14-month deadline left banks scrambling to address their electronic security tools.

Internet banking system offline for only a short period of time, Windham says. The real challenge, he adds, has been getting customers comfortable with the added security protocol.

First American National's customer base is divided between two groups: one that's in a more developed town and more computer-savvy and another that's more rural and less familiar with the Internet. To help the customers in this latter group adopt its question-based authentication system, the bank sent them letters in advance of the change and stuffed inserts in mailed statements advising clients of the specifics. Even with these measures, the new technologies still resulted in lots of extra call-center hours. Windham himself manned the phones to help field security-related questions.

"We've done a lot of one-on-one hand-holding," Windham says, such as helping users keep track of their security phrases and helping clients that have locked themselves out of their accounts after entering too many incorrect answers.

Like First American National, Farmer's National Bank, a \$398 million-asset bank located in Danville, Ky., rolled out a multifactor authentication security system that relies largely on challenge questions. The bank, which operates some of its electronic banking systems in-house and contracts some activities with third-party vendors, notified customers when the bank's added security protocols were about to come online, says Debbie Lowe, an associate vice president with the bank.

Farmer's National Bank has not experienced much resistance or confusion from its retail customers, Lowe says. The segment of the customer base that uses the Internet banking tools tend to be more Web-savvy and are comfortable with the increasingly common question-based routine, she says. "With all the stuff that is out there, customers are glad that they have a bank that's looking out for them," she says.

### **Not Done Yet**

Community banks and other financial institutions go to great lengths to fortify online security today, but future security improvements are likely to rely as much on customer education and vigilance as on actual technology advances. "You can use all the technology and fancy tools you want," Jaeger says, but he stresses that the best security "is transparent and relies on the good sense of the folks using it."

A recent Harvard/MIT study found that about 97 percent of banking customers forgot to check for their icons and phrases before entering a seemingly familiar site. Banks must view customer education efforts as an ongoing facet of their security activities,

**"With all the stuff that is out there, customers are glad that they have a bank that's looking out for them."**  
**— DEBBIE LOWE, FARMER'S NATIONAL BANK**

says Jaeger. Encouraging customers to check balances online often is key: Those customers that follow this practice have a higher likelihood of flagging suspicious activity and cutting off fraud, when compared to those who simply wait for monthly statements, he explains. Some banks have even adopted point systems that reward customers who visit their sites frequently.

In addition to using informational statements in mailers, Jaeger recommends hosting customers at branch events, such as a wine-and-cheese social, that feature a discussion of good online practices. Teaching such online practices is as important a security activity as implementing new software security systems, he says. "Fraudsters prey on the weakness of retail customers."

For online retail banking operations, most institutions have adopted some form of device identification—such as computer fingerprinting, IP address verification or encrypted cookie tools—and mutual authentication involving shared questions, says Michael Jackson, associate director of the Technology Supervision Branch for the Federal Deposit Insurance Corp., a member agency of the FFIEC.

These are economical and customer-friendly options, Jackson says, but the FFIEC realizes these solutions "are not a silver bullet."

Criminals, ever on the prowl, are sure to uncover vulnerabilities in these new solutions, requiring even more stringent identification requirements, says Jackson. "These solutions haven't been in place a year," he said. "It's still too early to say how particular solutions are vulnerable." **tb**

*Carli Flippen is a free-lance writer in Columbia, Md.*