



Security Vendors Look to Shield Business Accounts

American Banker | Monday, February 22, 2010

By [Daniel Wolfe](#)

Banks are not legally liable for fraud losses on business accounts, but some security vendors are focusing more attention there anyway.

"Banks are really concerned about the account loss, not necessarily the fraud," said [David Jevans](#), the chief executive of IronKey Inc., a five-year-old Los Altos, Calif., secure flash drive maker.

Businesses typically have stronger technological protections in place at their end, such as one-time-password-generating tokens, but have less legal protections; banks are not required by law to refund stolen funds to businesses, whereas they typically go above what the law requires in reimbursing consumers for any of their losses.

And even if a bank goes beyond what is required by law and makes a business customer whole, there is a good chance they may still leave the bank — and take hundreds of thousands of dollars in deposits, [Jevans](#) said. "Even if you reimburse them," those customers "know that they're vulnerable."

Because of this potential drain of deposits, banks are showing more interest in beefing up security for business accounts, especially as hackers get craftier about their techniques, he said.

IronKey was expected to announce today a USB stick that creates a secure online banking environment on business customers' computers. Within the virtual computer on that stick, a customer can visit only the legitimate online banking site — instructions could not be redirected to another machine or observed by viruses on the computer's primary operating system.

"What it looks like to you is ... the bank's Web site," Jevans said. "What it actually is, is ... a secure hardware environment running inside a window."

That secure environment runs Linux, a separate operating system not vulnerable to viruses written to run on Windows. The USB stick's software would also run a scan of the main operating system to determine if the user is infected, and pass that information along to the bank.

The devices could double as one-time-password-generating tokens for banks that use that system.

Other security vendors are also targeting business accounts. [Guardian Analytics Inc.](#) announced last week a version of its fraud-detection software designed specifically to address the techniques used against business accounts. It creates a behavior model of a company's typical online activity and compares new sessions against that; it also looks for specific behaviors that can be signs of imminent fraud, such as adding a new authorized user to an existing account.

Some businesses and government agencies that have been victimized by phishing attacks have been so upset with their banks' response that they took the matter to court. In one recent example, [Comerica Inc.](#) of Dallas has been sued by a Michigan metal supply company, [Experi-Metal Inc.](#), that alleges [Comerica's](#) security practices were insufficient in preventing phishers from stealing about \$560,000 by initiating dozens of wire transfers to foreign countries over the course of one morning.

Comerica has defended its security practices, noting that the wire transfers were authorized with the client's one-time-password token and that the banking company caught the wire transfers as they were occurring.

"Valid credentials assigned to an [EMI](#) employee were used to authenticate a log-on for purposes of online banking transactions," Comerica said in court filings. And upon noticing the strange transfers, "[Comerica Bank](#) initiated procedures to halt outgoing wire transfers on EMI's payment orders" and attempted to recover the money that was being sent away.

A Comerica spokesman did not return a call requesting comment for this story.

[Avivah Litan](#), a vice president and distinguished analyst at the Stamford, Conn., market research company [Gartner Inc.](#), said that many banks are likely to turn to stronger protections like what IronKey and [Guardian](#) offer because they do not want to lose more

business.

"The banks that are getting sued already made a calculated risk ... they know they're going to lose this customer, so they've already taken that into account" when deciding not to reimburse that customer for fraud losses, she said.

Whereas consumers are protected by law, "there's no law protecting business accounts," [Litan](#) said. "In the end, the bank's contract with the business is really what determines the protection."

Because hackers have already demonstrated their ability to thwart one-time-password devices, banks are looking into other methods of protecting account data. Both IronKey's approach of a protected virtual computer and Guardian's approach of stronger analysis could be effective means of improving security on business accounts, she said.

Ultimately, Litan said, more banks will choose to protect their customers than let them go. "I don't think any bank wants their customers to get their accounts raided," she said.

© 2010 American Banker and SourceMedia, Inc. All Rights Reserved.
SourceMedia is an Investcorp company. Use, duplication, or sale of this service, or data contained herein, except as described in the Subscription Agreement, is strictly prohibited.

For information regarding Reprint Services please visit: <http://www.americanbanker.com/aboutus/reprint-services-rates.html>