Banks run more than just security risk with single-factor authentication

November 23, 2009

As described in a previous Portals and Rails post, various reports have indicated that business customers' online banking credentials are being compromised and the fraudsters are performing unauthorized EFT transactions using either the ACH or wire transfers to move money out of these accounts.

This recent phenomenon could be seen as part of a larger issue for security on the Web, prompting some to consider whether online banking security standards are adequate.

While a lot has been written on how this fraud happens, not much has focused on what happens next. The criminal side of this is fairly cut and dry. Law enforcement tries to track down the fraudsters and bring them to justice. If the FBI, Secret Service, or other agencies are able to track them down, apprehend them, and a conviction is made, the fraudsters spend some time in jail. The civil side of this is a little more complicated.

One civil case that has gotten some recent attention is the Shames-Yeakel case filed in federal court in Illinois. Marsha and Michael Shames-Yeakel had $26,500 stolen when an unknown person gained online access to the Shames-Yeakels' bank accounts by using Ms. Shames-Yeakel's username and password. The thief manipulated a line of credit and subsequently wired the funds out of the Shames-Yeakel's business account to Hawaii and then off to a bank in Austria. While there is probably a good joke about yodeling while playing the ukulele buried in all of this, the Shames-Yeakels are not laughing. In fact, the hills are alive with litigation.

The plaintiffs first turned to their bank, who indicated that under the bank's online banking agreement, the plaintiffs were responsible for the lost funds. They next turned to the Office of Thrift Supervision (OTS), the bank's primary regulator, seeking protections under Regulation E and Regulation Z. The OTS found that these regulations did not apply as they were applicable to consumer loans and lines of credit.

Ultimately, the Shames-Yeakels sued their bank. The legal viability of their claims was considered by the Court in its Aug. 21, 2009, ruling on the bank's motion for summary judgment.

While the court's opinion addressed a number of legal claims, it is the court's ruling on the plaintiff's negligence claim that bankers should pay close attention to. The basis of this claim is that the bank and its third-party Internet banking service provider did not follow the Federal Financial Institutions Examinations Council (FFIEC's) updated 2005 guidance on authentication in an Internet banking environment. At the time of the incident, the bank had user name and password access to their online banking system. The FFIEC's guidance does not require banks to use dual-factor or multi-factor authentication for these accounts, but it does state that the federal regulatory agencies consider single-factor authentication, like user

name and password, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. In essence, the court indicated that while the facts must still be weighed by a jury, it declined to dismiss a negligence claim that the bank had breached a duty under Indiana law to protect the confidential information of its customers by failing to implement more robust security systems. The court stated: "In light of [the bank's] apparent delay in complying with FFIEC security standards, a reasonable finder of facts could conclude that the bank breached its duty to protect Plaintiffs' account against fraudulent access."

Another case to keep an eye on was filed in Maine this past September. The case involves a Maine based construction company, Patco, who is suing its bank for $588,000; the same amount of money that was stolen from Patco's account over the course of an eight day period in May. Similar to the Shames-Yeakel case, Patco is claiming that the bank failed to provide commercially reasonable protection because only a single-factor authentication system for its online banking system was in place. While no action has been taken as of yet, it will be interesting to see if the state court in Maine agrees that with the U.S. District Court in Illinois, allowing this negligence claim to move forward.

By guest blogger Michael T. Stewart, assistant vice president at the Boston Fed

- November 23, 2009 in
  - ACH
  - identity theft
  - payments risk
- Permalink
- Comments