KrebsonSecurity
In-depth security news and investigation

Missouri Court Rules Against $440,000 Cyberheist Victim

By Brian Krebs | March 26, 2013

A Missouri court last week handed a legal defeat to a local escrow firm that sued its financial institution to recover $440,000 stolen in a 2009 cyberheist. The court ruled that the company assumed greater responsibility for the incident because it declined to use a basic security precaution recommended by the bank: requiring two employees to sign off on all transfers.

Springfield, Mo. based **Choice Escrow and Land Title LLC** sued Tupelo, Miss. based **BancorpSouth Inc.**, after hackers who had stolen the firm's online banking ID and password used the information to make a single unauthorized wire transfer of $440,000 to a corporate bank account in Cyprus.

Choice Escrow alleged that BancorpSouth's security procedures were not commercially reasonable. Choice pointed out that the bank's most secure option for Internet-based authentication relied principally on so-called "dual controls," or requiring business customers to have one user ID and password to approve a wire transfer and another user ID and password to release the same wire transfer.

Choice Escrow's lawyers argued that because BancorpSouth allowed wire or funds transfers using two options which were both password-based, its commercial online banking security procedures fell short of 2005 guidance from the **Federal Financial Institutions Examination Council** (FFIEC), which warned that single-factor authentication as the only control mechanism is inadequate for high-risk transactions involving the movement of funds to other parties.

But in a decision handed down on March 18, 2013, a judge with the **U.S. District Court for the Western District of Missouri** focused on the fact that Choice Escrow was offered and explicitly declined in writing the use of dual controls, thereby allowing the thieves to move money directly out their account using nothing more than a stolen username and password. The court noted that Choice also declined to set a limit on the amount or number of wire transfers allowed each day (another precaution urged by the bank), and that the transfer amount initiated by the thieves was not unusual for Choice, a company that routinely moved large sums of money.

Like most U.S. states, both Missouri and Mississippi have adopted the Uniform Commercial Code (UCC), which holds that a payment order received by the [bank] is "effective as the order of the customer, whether or not authorized, if the security procedure is a *commercially reasonable method* of providing security against unauthorized payment orders, and the bank

proves that it *accepted the payment order in good faith* and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer."

The Choice Escrow judgment may be among the first to focus on a particular aspect of the UCC (Article 4a), which states that if the bank offers to the customer a security procedure which the customer declines, the bank can argue that its procedures were commercially reasonable, said **Dan Mitchell**, an attorney in Portland, Me.

"Really, it looks like that's what this whole case was about for the court, which didn't examine whether the bank's security procedures were commercially reasonable," said Mitchell, who recently represented **Patco**, a Maine construction firm that successfully sued its bank for poor security following a $588,000 cyberheist that also took place in 2009. "The court's whole analysis was about the fact that the bank offered dual controls which the customer declined."

Charisse Castagnoli, a bank fraud expert and independent security consultant, said the fraud incident happened before banking regulators issued the current online banking security guidelines, which call on banks to take additional steps to protect customers from account takeovers — including educating customers about the sophistication of today's threats.

"The bank's security may not have been sufficient by today's standards, but the key here was that the bank offered a security measure that was refused," Castagnoli said. "If the bank doesn't ever make the recommendation to use additional controls, then shame on them. But in this case, it seems like the bank was trying to steer their customer to use those controls. Considering this was back in 2009, it looks like the bank was at least doing a pretty good job informing their customers about the need for dual controls."

Choice Escrow declined to comment, or say whether it planned to appeal. But according to Castagnoli, summary judgments can be difficult to appeal. "It's pretty expensive, and the standard of review for the court is fairly high."

There is no doubt that requiring two employees to sign off on all transactions minimizes the potential for fraud (particularly employee/insider fraud). But dual controls alone are hardly sufficient. The very first cyberheist case that I wrote about — back in the summer of 2009 — dealt with the electronic theft of $415,000 from Bullitt County, Kentucky. Bullitt had set things up so that all payments had to be initiated by the county treasurer and approved by the county judge.

In that attack, the crooks had compromised the treasurer's computer, which allowed them to change the email addresses that were to receive notifications about new transactions. They were able to do this because the treasurer was the designated administrator of the county's account settings at the bank. They then changed the judge's password in the bank's system, and approved the fraudulent transfers using a computer outside of the state of Kentucky.

The best way to avoid a cyberheist *is to not have your computer systems infected in the first place.* The trouble is, it's becoming increasingly difficult to tell when a system is or is not

infected. That's why I advocate the use of a Live CD approach for online banking: That way, even if the underlying hard drive is infected with a remote-access, password stealing Trojan like **ZeuS** or **Citadel,** your online banking session is protected. This is just one of the tips from a much longer list of precautions that small- to mid-sized businesses should consider adopting when banking online.

Dan Mitchell is a shareholder and a member of Bernstein Shur's Litigation Practice and Data Security Team. He can be reached at 207-228-7202 or dmitchell@bernsteinshur.com.