



TEXAS BANKERS ELECTRONIC CRIMES TASK FORCE



Bulletin 2013-1

April 22, 2013

The following is a recent action or issuance to be considered in the risk management practices for reducing the risks of Corporate Account Takeovers through the Protect, Detect, and Respond framework.

Court Favors Bank in Fraud Dispute **Judge: Choice Escrow Declined Bank's Dual Controls**

A U.S. District court in Missouri recently issued a judgment in favor of a financial institution in a cybercrime dispute from 2009. Choice Escrow and Land Title LLC (Choice) sued BancorpSouth, Inc. to recover \$440,000 which was wired to an overseas account in Cyprus after hackers had stolen the firm's online banking ID and password and used the information to make a single unauthorized wire transfer. 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. The judge determined that refusal by the company relieves the bank of responsibility for the losses that later resulted.

The court's decision is supported by a provision within the Uniform Commercial Code's (UCC) Article 4A that governs how financial institutions should handle incidents of wire-transfer fraud. The court notes that if a bank offers security procedures that a commercial customer refuses, then according to that UCC provision, the customer is liable.

Recommended Action:

It is unfortunate when any financial losses occur, especially of this size. No one wins but the thieves. Both the customer and the bank will suffer reputation damage within their community at a minimum.

As required by Supervisory Memorandum 1029, issued by the Department of Banking on January 9, 2012, banks need to educate their customers on CATO risk.

If a customer is unwilling to adopt appropriate security practices, a bank has two choices:

- 1) Terminate the banking relationship to avoid potential reputation damage if a theft occurs, or
- 2) Continue the relationship without the use of security practices and run the risk of litigation if a theft occurs.

Should the bank choose the latter, this court case illustrates that if a bank is diligent in documenting repeated offers to the customer for stronger security and documents the customer's refusal of the offers (including getting the customer's written acknowledgment that they are assuming all risks for transfers initiated in their name), a court is more likely to rule in the bank's favor.

While it is not common for a commercial customer to refuse security features, documenting such a decline is critical. Most importantly, banks should be proactive in educating corporate customers about cyber risks and offering them the tools to mitigate it.