



TEXAS BANKERS ELECTRONIC CRIMES TASK FORCE



Bulletin 2012-4

April 5, 2012

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.

Cyber Thieves Capture Telephone Information and Block or Divert Calls to Corporate Customers

Cyber thieves are capturing telephone account information belonging to their victims. The goal is to enable the attackers to either block or divert calls from the bank to the corporate customer when a theft is in progress.

Recommended Action:

Customer cell phone numbers are sometimes used by the bank as an alternate contact to discuss suspicious transactions or for sending out-of-band communications (such as a one-time password).

If customers have provided their cell phone and it is listed in their on-line banking account information, you should presume that the thieves know that number and might block or intercept communication to your customer. Make your bank staff aware that if they are unable to reach the customer, thieves might be blocking communications to the customer's telephone line (and email). If you use customer cell phones for out-of-band communications, and especially for one-time passwords, re-evaluate all elements related to this practice to determine if any controls need to be modified.

Notify customers of this new development. Alert them to contact the bank if they see a pop-up box asking them to update their contact information (phone numbers) at any time, even if the pop-up box occurs just after they have logged in to an on-line banking session. Additionally, establish procedures (or an understanding) with the customer regarding what actions the bank will take if the bank cannot confirm a transaction that it finds suspicious.