PROTECTING AGAINST BANK FRAUD

by Steve Brown

You may be shocked to hear it, but according to the Association of Certified Fraud Examiners, 86% of people found to be perpetrating fraud in business had never been charged with a prior offense. In banking, fraud can take have many varieties - from submitting false loan applications, to lying about income, forging bank statements, forging tax returns or siphoning money out of accounts belonging to senior citizens. A survey outlined in Bank Information Security found that over 55% of small businesses surveyed in fact, had experienced a fraud attack in the prior 12 months. The root problem is that banks, as infamous bank robber Willie Sutton said, are where the money is. Unfortunately, anytime you find money and combine that with a stressed economy, fraud is likely to follow. To protect customers and banks, here are some tips.

Identity Theft - criminals typically steal personal information through a variety of sources, such as a wallet, digging through trash, or compromising credit or bank information. It is important that bankers warn their customers that information about them is so numerous, they cannot prevent identify theft, but they can minimize the risk of loss simply by doing a few key things. For instance, warn customers never to throw away ATM receipts, credit card or bank statements without shredding them; never give a credit card number over the phone, unless the customer originated the call; reconcile accounts monthly and alert the bank to any discrepancies when detected; keep a list of phone numbers to call to report theft; review credit reports at least 1x per year; and report mail received from credit card companies or banks in someone else's name to law enforcement.

Prime Bank Note Fraud - here, "bank guarantees" are pitched that can be bought at a discount and sold at a premium. To sink the hook even further, crooks use legal documents that require victims to enter into non-disclosure; non-circumvention with a goal is to get the victim to send money to a foreign bank. To avoid this, warn customers to think before investing in anything; be wary of any opportunity that offers high yields; and independently verify the identity of the people involved.

Email fraud through ACH/wire transfer - here, criminals target businesses that post jobs online, by introducing malware into an email in response to the job posting. The attacker then obtains online banking credentials of the person who was authorized to conduct financial transactions within the business, changes account settings and sends wire transfers or ACH. In a variant on this theme, thieves target senior executives or accounting and HR personnel specifically with a goal of stealing personal information and log-in credentials. To avoid this, warn customers to remain vigilant in opening e-mails of prospective employees; run a virus scan prior to opening e-mail attachments; and use separate computer systems to conduct financial transactions.

Customers trust their banks, so watching out for them is just part of the job. Sometimes the statistics can be startling, so getting the word out is critical. For instance, studies find 73% of people use their online banking password at non-financial web sites; 49% of victims do not know their information has been stolen; 26% are alerted to suspicious account activity by credit card issuers or banks; 19% report checking or savings accounts were misused; and 4% of information comes from stolen mail. One final thing - research firm Celent finds insider fraud accounts for 60% of bank fraud cases where a data breach or theft of funds has occurred. Sometimes, just knowing the information can help.

BANK NEWS

White House White Paper

The much anticipated "White Paper" on the GSEs was released and it was surprising for its lack of conclusions. The 31-page report outlined 3 options: 1) A privatized system with very limited Gov't backing and a focus on low to moderate income households; 2) A privatized system with a "springing guarantee" that increases Gov"t support in times of crisis; and 3) A reduced structure whereby the Gov"t only participates in catastrophic reinsurance. Few details were offered and the Paper stopped short of recommending any option. In short, the Paper will do little to help the debate, but supports the notion that the Gov"t should take a reduced role going forward (look for higher guarantee fees to start, lower limits and smaller portfolios). It should be noted, however, that the Paper commented that the FHLB system worked well during the crisis and shouldn"t be touched (it did note however that banks should only be a member of 1 FHLB and borrowings should be limited in size for each bank).

Closed Banking

A study by Bank Systems and Technology finds 64% of people say their primary bank has a good reputation, but 40% don't think their bank looks out for their interests. In addition, 92% said their bank was innovative; the same percentage said it offered high quality online or web based payment banking services; 93% said their bank was trustworthy; and 70% were unsure whether their bank offered RDC through a mobile application. Get the word out.