ARRESTING ID THEFT

by Steve Brown

Given that 68% of independent banks expect to increase their internet capabilities in 2007, it makes sense that they should also devote more resources to educating customers. Since the internet sharply reduces a bank's cost of delivery, it is in our own collective best interest to ensure customers continue to feel safe and secure. Here are a few quick things banks should know related to ID theft. The number one way ID theft occurs (30% of cases) is through lost or stolen wallets, checkbooks or credit cards. Studies show that 90% of compromised data still happens through traditional offline channels and not through the internet. About 50% of all ID theft is perpetrated by friends, neighbors, employees, family members or relatives. It takes about 40 hours for a victim of ID theft to clean up the mess, a 21% jump over the past 3 years. Approximately 11% of fraud cases are caught via credit monitoring reports. Given that information, here are a few best practice suggestions culled from our banks. Banks should consider working the following points into customer education marketing collateral. 1) Never release Social Security or account numbers in response to e-mail or phone requests. Banks should notify customers through various channels (email, posted placards in the branch, etc.) that they would never ask for any account details or verification through an email. 2) Keep all sensitive documents, checkbooks and credit cards securely locked up and only carry the minimum number of credit cards needed. 3) Provide customers with a call in number to verify requests purporting to be from the bank. 4) Use an alphanumeric scheme in documents used in marketing campaigns so the bank can quickly reference materials and determine whether or not they are legitimate. 5) Remind customers to review bank statements online every 2 weeks. 6) Market direct deposit and automatic payroll as a theft reduction opportunity. 7) Customers should also be prompted to keep passwords hidden, change them frequently and to shred all private documents. 8) Educate customers how to use the bank's web site to monitor account activity. A study done by the Better Business Bureau found that people who access accounts online detect crime earlier (22 days vs. 67 days) than those who rely only on mailed monthly paper statements. The study also found that victims of ID theft who detected the crime by monitoring accounts online experienced financial losses that were less than 1/8 of those who detected it via paper statements. In addition to keeping customers safer, this has the added benefit of training customers to use your online services Â– a less expensive product delivery channel. 9) Other ideas include offering ID theft protection with accounts, contacting the bank if statements aren't received and providing tips on how to get Microsoft security updates. 10) Finally, some banks are even giving away firewall software. This is not shocking, as a recent study found an astonishing 67% of people do not have firewall software installed on their computer and 58% couldn't explain the difference between firewall and antivirus software. Finally, some banks are going with an email-based alert system that monitors transfers, payments, balances, withdrawals, and detects out-of-pattern activity. Educating customers is critical to protecting them. In an effort to build customer loyalty and raise the education level, bankers may want to consider updating marketing collateral on simple ways customers can protect themselves against ID theft.

BANK NEWS

M&A

Sandy Springs Bancorp ($2.6B, MD) will purchase Potomac Bank of VA ($247mm, VA) for $64.7mm in cash and stock, or almost 2.63x book.

M&A

Washington Federal ($8.8B, WA) will acquire the holding company of First Federal Bank ($561mm, NM) for $99mm, or about 1.76x book.

Bies on Risk

Fed Governor Susan Bies (voter) urged banks to improve their financial risk management methods and warned that the current "relative calm" may not last. Bies said that banks need to ensure that "capital is strong enough to support the bank" under an extended credit shock scenario.

FDIC Surplus

A one-time credit of $4.7B will be used to offset future FDIC assessments for institutions that paid assessments prior to 12/31/96.

The Fed on Electrons

Fed Vice Chair Kohn said the growing use of debit cards and electronic check payments is altering how the Fed processes payments for banks. Kohn said check processing centers are shrinking and will be down to 1 within 10Ys. He also said electronic processing will allow for greater availability of funds and cheaper transactional costs for banks.

Florida

The state reports that for the 12 months ended 8/31/06, condominium sales were down 41% statewide. In addition, single family home sales dropped 34%.

Money Transfers

The Fed has set up its "Directo a Mexico" program that will allow commercial banks to move money for Mexican workers though the Fed's ACH system. The goal is to provide a safer money transfer system at about 35% of the cost than Mexican workers currently pay at non-banks.

Spending

An economic survey estimates consumers will spend over $4.9B this Halloween, up a dramatic 50%.

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.