BANK TO CYBER THEFT SCHOOL

by Steve Brown

As summer winds down and families everywhere think about hitting the stores to spend money on back-to-school shopping, it might interest you to know how such money is typically spent. A survey by the National Retail Federation finds parents will spend an average of $603.63 for kids K-12. By major category, about 15% is spent on actual school supplies, 17% goes toward new shoes, 31% is spent on technology and 37% is spent on clothing. Given so much money is being used to properly attire kids, it might make sense to attach an alarm system to the backpack to avoid any potential for theft at the school. Speaking of protecting your bank against the potential for theft and where to spend money, we focus our energy today on the risk of cyber threats. Consider a recent Fed analysis that found phishing attacks alone had jumped from 16,247 per month back in Sep. 2010, to 38,970, as of the same period in 2011. That is about a 240% increase in 12 months and it shows more must be done to protect the bank and its customers. In addition, the data also shows 29% of online internet users have been a victim of a phishing attack and the average amount stolen per consumer per attack is $352. That adds up to a whopping $1.3B in total global losses just in 2011 alone. In response to this risk and increased concern, regulators are ramping up requirements around cyber threats to banks. Regulators now expect banks to have layered security (where different controls occur at different points in a process) for consumer and commercial accounts. Examples of layered security include fraud detection and monitoring systems that take into consideration the customer's history and behavior; dual customer authorization through different access devices; out-of- band verification for transactions; "positive pay," debit blocks, or other techniques to limit the transactional use of an account; enhanced controls over account activities; adding transaction value thresholds, payment recipients, number of transactions allowed per day or allowable payment windows on specific days or times; using internet protocol tools to block connections to/from unknown IP addresses or those suspected to be associated with fraudulent activities; and beefing up policies around customer devices that could be compromised. Further, banks should have anomaly detection and response processes in place to handle initial customer login and at the initiation of any funds transfers to other parties. For commercial accounts in particular, regulators expect even greater risk controls to be in place (larger dollar amounts and more frequent funds transfer activity). Finally, use multifactor authentication whenever possible, as you enhance controls for customer administrators (as well as user access privileges). In addition to all of these items, customer education has become more important. While this allows you an opportunity to differentiate your bank from others and to seize on cross sell opportunities, it also requires a consistent and thorough approach when it comes to online banking security. Here, banks should educate customers on how to implement electronic banking controls, information security controls, perform risk assessments and even to help them better understand Regulation E (electronic funds transfers) protections and limitations. When doing so, be sure to give your customers bank contact information that can be used in the event a customer uncovers suspicious activity or has a security issue. At a high level, as the environment has changed and so too, have regulatory expectations. As such, any time a customer conducts an electronic transaction where it accesses customer information or moves funds to other parties, an extra level of security is expected. A good rule of thumb to use is that the riskier the transaction, the more regulators expect your bank to increase controls around each transaction.

BANK NEWS

Closed (40)

Regulators closed 2 branch Waukegan Savings Bank ($89mm, IL) was closed will almost all the assets and deposits were assumed by First Midwest Bank ($7.9BB, IL).

M&A

City Holdings ($2.9B, WV) will purchase Community Financial ($504mm, VA) in an all-stock deal worth an est. $26.1mm, or approx. 55% of book.

Expanded Zillow

Real estate valuation firm Zillow announced it will release a set of tools created for real estate agents that will allow integrated valuations, listings and contact management. The targeting of businesses is a change in their past business model and could include banks in the future.

New Fed Chair?

A Reuters profile article on Vice Chair Janet Yellen speculates she is the favorite for a President Obama appointment when Bernanke's term expires in Jan. of 2014 - of course there are lots of assumptions made here obviously.

Student Loans

Suntrust introduced a new student loan consolidation refi product that has both fixed and variable rate options. Suntrust will use First Marblehead's technology and servicing platform to handle the workflow.

FSOC Regulation

The Fed approved a final rule related to the supervision of financial market utilities designated as systemically important. The rule establishes risk management standards and sets requirements and procedures.

Home Ownership

The Census Bureau reports 2Q home ownership was 65.5%, up slightly from the 65.4% level of 1Q (the lowest in 16Ys), but down from the 65.9% level of 1Y ago. The highest rate was in the Midwest (69.6%) and the lowest was in the West (59.7%). Meanwhile, those 65Ys+ have an 81.6% ownership rate.