Staying Healthy In A Fraud-Driven World

by Steve Brown

This year's flu season was expected to be bad and it is mostly living up to that expectation. Even those who have been vaccinated are at risk, because of mutations in the virus that came about after the vaccine was designed. Even so, health officials say it still pays to get vaccinated, as it's the best way to reduce the chances you'll get the flu and spread what can be a deadly disease.

Wouldn't it be nice if there was a vaccine to protect banks from credit and debit card fraud? Certainly 2014 was a bad year for card breaches, as a number of large consumer brands found themselves in the hot seat. Banks, meanwhile, were left to pick up the pieces. The number of credit and debit cards compromised in data breaches reached 64.4MM in 2014, up 38% from 46.6MM in 2013, according to the Identity Theft Resource Center. Consider that as a result of the Home Depot breach alone, community banks reissued nearly 7.5MM credit and debit cards at a total cost of more than $90MM, according to ICBA.

Last year around this time, the ICBA published information on some key considerations for banks facing payment card compromises. There's no reason to suspect the thieves will be going underground any time soon, so as 2015 gets off to a fresh start, we thought we'd revisit these recommendations as a booster shot of sorts for community banks.

For starters, it's important for banks to continually troll the popular press for information from compromised or potentially compromised companies. You've got to try to understand the extent of the breach and whether there is a known fraud pattern. Also be sure to quickly review all fraud alerts from your payment card network/processor and keep on top of situations as they continue to unfold. It's also a good idea to beef up monitoring on cards that could be affected by a breach.

When a breach situation occurs, you'll need to consider the decision whether or not to reissue cards. There can be issues with counterfeit fraud insurance coverage if you opt not to block and reissue new cards. On the other hand, it may be enough to issue the same card with a different expiration date and CVV.

Of course, you also need a solid plan for responding to questions from customers. That means your staff has to be prepared to answer questions and help customers understand that they won't be liable for fraudulent charges. Customers should also be reassured that the bank has multiple layers of security to protect their personal information.

It's also a good idea to be proactive with customers, to help them understand how to best keep their data secure from unwelcome intruders. This can include informative bank signage and periodic email reminders about how to spot scams or hints on how to protect personal information. For instance, most customers now know to cover up the key pad as they enter their pin at an ATM. But these same customers may not be aware of the need to protect their personal information when they apply for cards at a department store or retailer. There's a very real danger that a thief could be lurking over one's shoulder, snapping pictures of the application with a cell phone.

The bad guys aren't going away, so it is all the more imperative for banks to step up to protect themselves and their customers from unhealthy complications associated with credit and debit card fraud.

BANK NEWS

Good News

China's central bank has cut bank reserve requirements in an effort to flood the system with liquidity and boost the economy. The move pushes about $96B US back into the economy.

Disclosure Changes

The Financial Times reports the Basel Committee will move forward with a plan to overhaul reporting standards for the banking industry in an effort to make sure banks are more consistently and transparently disclosing balance sheet risks.

Investigation

Bloomberg reports the DOJ is investigating Rabobank Group over potential AML deficiencies.

Small Biz

A survey of small businesses by Wasp Barcode Technologies finds: 57% predict revenue growth this year; 38% plan to increase IT spending; 23% do not know how much revenue they generate online and 57% generate less than 20% of their revenue online.

Rising Defaults

Moody's reports about 39% of companies that defaulted from Q3 2010 to Q3 2014 did so more than once vs. a 17% average that did so since 1987.

Asking Permission

Regulatory rules require banks to alert regulators when directors or senior executive officers change at a time when the bank is not in compliance with minimum capital requirements; is in troubled condition; or is working under a capital restoration plan. The notification should include a copy of the position description, a description of the nominee's qualifications for the position, a biography, financial information, fingerprint cards and a completed IRS Tax Check Waiver form as may be appropriate or required. We bring this up because so many bankers have moved around over the past few years following the crisis and because the average age for bank directors is reportedly just over 67Ys old according to surveys.

Stressful Situation

A Pew survey finds the typical middle class family could only replace 21 days of income with readily accessible funds. What is even scarier perhaps is that the same survey found that even if these families liquidated all of their retirement savings and investments they could only replace 119 days of income.