Never Ending Battle Against Fraud

by [Steve Brown](#)

Illusionists and magicians can be really interesting to watch as they use sleight of hand and other techniques to fool audiences. One persistent rumor in such circles is that Harry Houdini, the famous illusionist and stuntman, died when one of his spectacular performances went horribly awry. In reality, however, the 52-year-old performer died of peritonitis from a ruptured appendix on Halloween in 1926. The myth of his alleged drowning in his Water Torture cell, originated from a 1953 film that depicted his death in this more dramatic and patently false manner.

In the banking industry these days it can also be hard to know what's true and what isn't. We recently came across some data that suggests nearly 50% of Americans have had personal information compromised in the past year. Whether you are dealing with malicious software, Phishing schemes, distributed-denial-of-service attacks, credit card fraud or something else equally bad, it seems there's no end in sight to thieves trying to worm their way into areas they don't belong.

Given so much fraud out there, it's particularly important for banks to remain vigilant and to keep customers informed. The good news is that research shows banks are successfully warding off a good portion of attacks. In 2012, for instance, banks stopped $9 out of every $10 of attempted deposit account fraud, according to an ABA study. The bad news is that it seems likely the stakes are going to continue rising so banks are going to have to work even harder.

Congress for its part is also taking a greater role amid widespread security breaches in the retail space. Banking regulators too expect banks to circle the wagons, taking an even more proactive in quashing fraud. The FFIEC and the OCC have already been forthcoming on plans to beef up cybersecurity oversight on community banks this year so get prepared no matter whether you run core systems yourself or you outsource them. You must be prepared to substantiate what you are doing to fight fraud and show your efforts are coming from the executive level on down through the entire bank.

Meanwhile, many community banks feel stuck between a rock and a hard place when it comes to adequately raising cyber shields. Many feel they are at a disadvantage because they don't have the money or resources big banks have to fight fraud. Yet it seems clear that regulators plan to hold everyone accountable.

When it comes to fighting fraud, there's safety in numbers so community banks might find it helpful as a starting point to join groups such as the Financial Services Information Sharing and Analysis Center. This group helps quickly disseminate physical and cyber threat alerts and other critical information to its members so it may be of help.

Further, community banks must do their best to stay abreast of emerging technology that can help you combat fraud. Just recently, for instance, Apple said it was going to allow third-party developers to build upon its Touch ID authentication system. This could be very useful to banks in adding a layer of customer protection using fingerprints and a smartphone to authenticate users. While the whole area of biometrics is still in the embryonic stages, be sure to keep a close eye on developments as you consider how these technologies could be implemented.

Cost is certainly an important factor to consider along the way, but so too is the regulatory push to hold banks more accountable for fraud-fighting efforts. To avoid regulatory pressure, dispel yourself of the illusion that you can simply will away these problems or that they are the issue of an outsourcer and not yours. These are your customers, so regulators want to see you working diligently to protect them as you try to avoid the cyber magicians trying to sneak in with their smoke and other tricks.

BANK NEWS

Less Traffic

Fifth Third projects branch traffic will decline 20% this year.

Branch Visits

The ABA reports Synergistics Research estimates the frequency of branch visits has declined 36% over the past 18Ys (from 4.4x per month in 1995 to 2.8x in 2013).

Risky

A 3Y survey of Millennials (18Y to 34Y) finds 33% say they are open to changing their bank in the next 90 days and the same percentage say they don't think they will need their bank at all in the next 5Ys.

Universal Tellers

The ABA reports tellers earned an average of $25k in 2012 and universal bankers earned 50% more.

Fraud

A survey by Kroll finds 75% of financial services firms globally reported a fraud in the prior year and 29% reported an internal fraud.

Failures

SNL Financial reports 16% of the banks that started between 2000 and 2006 failed. Meanwhile, the number of banks started over the past 5Ys has been 23 (20 in 2009, 2 in 2010, 0 in 2011 and 2012 and 1 in 2013).

Mobility

A comScore report finds smartphones and tablets combined now account for 60% all online traffic, 23% of organic website traffic now comes from a smartphone (12% comes from tablets), 20% of total digital time spent is on social networking (#1 category and 70% comes through mobile).