Assisting Customers While Assisting Your Bank

by Steve Brown

A Wells Fargo/Gallup poll of US adults finds 32% are providing assistance to an adult child, parent or both. Of this group, 75% were doing so to assist an adult child, 19% were helping a parent and 6% were assisting both. In addition, the survey found 46% of respondents overall, who have one or more grown children, said they were providing them with financial support. This could provide an opportunity for your community bank so we thought you might want to know.

Another thing to know this morning relates to wire transfer fraud. On this front, the FBI warns wire transfer fraud is rapidly rising, as cybercriminals use a combination of sleuthing skills, social engineering and basic hacking to siphon money from trusting banks and business executives.

According to an FBI report, hackers aimed to steal more than $2.2B through wire fraud known as business email compromise, in the last half of 2016. This amount represents more than 67% as much attempted wire-fraud thievery as was committed in the previous 2.5Ys combined. Further, the actual number of reported cases doubled, which points to more hackers seeing the benefits of this type of fraud, so all bankers should be on alert.

In such scams, what appears to be a legitimate email from a top executive (often the CEO) arrives in the inbox of someone working in finance or accounts payable. The email indicates a wire transfer must be issued immediately and that the executive is in some situation that adds pressure to make things happen fast.

As if that weren't enough, the email address will usually appear as a legitimate company email and will often include references or details that (seemingly) would verify that the request is coming from the actual person. In reality, such details are often gathered from the dark web, social media accounts, or the company's own website.

Then, with a directive in hand, from what appears to be a high-ranking company executive, the recipient will process the transfer as requested in the email. Once the money is wired out of the country it disappears into the mist.

Meanwhile, another survey by the Association for Financial Professionals finds 74% of respondents reported their organizations were exposed to either attempted or actual payments fraud in 2016. This percentage is a record high since 2005, when the survey was started.

The same survey also found that wire transfer scams topped the list, ahead of ransomware, tax phishing and tech support scams. Clearly, cybercriminals opt for this scam because it offers a quick, healthy payoff that is faster than ACH or check fraud. It also offers the criminals a very low risk of getting caught.

Since these incidents can not only be costly, but embarrassing to the companies and executives involved, industry experts believe many of these scams go unreported. As a result, the FBI numbers may show only the tip of the iceberg on such crimes.

We note as well that these wire transfer scams have also given way to similar scams aimed at gathering employee tax information or W2 records. In this way, fraudsters can file a fake return and collect refunds.

Your bank and your business customers are of course not immune to such risks, but more can always be done. Certainly, making sure your staff is well trained on the protocols for any wire transfer requests AND follows those explicitly (about 95% of scams are due to human errors), will help protect you.

Just as important is educating your business customers on these scams. It will help keep them out of harm's way and reduce their risk profile over time. That is good for you too, because they likely are your biggest risk issue so arming them with information can be a good thing.

Lastly, it goes without saying, but the least amount of personal information available on your executives, especially travel plans, the better. After all, you wouldn't want to throw a life preserver to these criminals that help them float away with your money.

BANK NEWS

Savings

A Princeton Survey Research Associates International survey finds more than 30% of Americans have saved enough money to cover 6 months' worth of expenses, marking a 7Y high. At the other end of the spectrum, 24% said they had no savings, a 6Y low. Unfortunately, Bankrate research finds 32% of those ages 53 to 62 said they have nothing saved, which is more than any other group.

Strategic Risk

Regulators indicate strategic risk is the appropriate governance in the bank's decision-making process and implementation of decisions. Doing so incorrectly can result in missed business opportunities, losses, failure to comply with laws and regulations resulting in civil money penalties (CMP), and unsafe or unsound operations that could lead to enforcement actions or inadequate capital.

Shifting Usage

Research by PwC discovers only 10% of customers now use human interaction channels such as branches, call centers or text vs. 15% just 5Ys ago. Meanwhile, over that same period online, digital and mobile usage has jumped from 27% to 46%.

Access by Type

An FTC study that looked at how hacked consumer data is used finds the top unauthorized access attempts by account type focus on email services (96%), credit card numbers (96%), and payment accounts (90%).

DEPOSIT OPPORTUNITIES

In an effort to expand our relationships, PCBB is pleased to offer community banks a money market deposit account rate of 1.10%, subject to availability. Contact operations@pcbb.com