Fighting Back Against Financial Scams

By Charlee Beasor

There may be no better real-life analogy on the topic of combating financial fraud than Andy Shank rescuing this writer from an underpass in a thunderstorm after my car battery died on the way to meet him to discuss his role as a professional fraud investigator.

Because with financial fraud, when (not if) it rains … it pours.

And if you're caught unprepared without appropriate technology safeguards and employee policies – like I was caught in a rainstorm without an umbrella and in impractical shoes – the damage is more than just wet clothing; your company and customers are at risk.

That's where professional fraud investigators like Shank come in. As assistant vice president of fraud investigation manager at Elements Financial, he's investigating and battling fraud to protect the financial institution and its customers.

As a former detective with the Indiana State Police (ISP), he's spent over a decade rescuing people stranded on the side of the road and in other situations. Shank was appointed to the Federal Bureau of Investigation to work on mortgage fraud and other white collar crimes and investigated several local high-profile cases: financier Tim Durham, former lawyer William Conour, the Indy Land Bank scandal and many others.

Shank emphasizes that fraud is no small matter and often the money goes to support organized crime or terrorism. He's learned that firsthand at Elements.

"I'm of a basic thought that we're all in somebody's hopper. We're in somebody's inbox to have damage done to our identity. We've all been in (cybersecurity data) breaches, we've all had our data compromised," he says matter-of-factly. "It's just a matter of when the bad guys get around to you in their inbox."

A hole in the armor

Fraud goes back to the dawn of time. "Con men" have been scamming people out of money and possessions for ages. The premise of fraud is the same as it always has been, though tactics have changed as technology has progressed.

EY (formerly Ernst & Young) offers clients auditing, advisory and consulting services, including fraud prevention and cybersecurity consulting.

"There is not a one-size-fits-all kind of concept. What we do for our clients, we investigate these complex cyberbreaches, help remediate those; and unfortunately, if those happen we help them learn from the mistakes," says William Knerr, partner at EY in Indianapolis.

EY advises clients that cybersecurity is a top risk for all businesses. Knerr acknowledges how fraud has evolved over time to include not just a phishing scheme for money, but shutting down businesses, taking data hostage and stealing proprietary information.

"You may not lose a single dollar, but you may lose trade secrets that haven't been patented yet," he states.

Additional fallout includes companies being subject to lawsuits or legal fees, as well as brand damage.

Several major brands are still reeling from – and paying for – financial breaches over the last few years. Target's 2013 breach affected 41 million credit cards and was caused by hackers compromising a third-party vendor; the company settled in 2017 for $18.5 million. A 2014 data breach at Home Depot affected 56 million credit cards and will end up costing the company at least $179 million.

"It's very difficult to quantify (the cost to business). A lot of places try to keep it under wraps. If they pay a ransomware and by some miracle somehow get their data back, they're

The financial industry is a common fraud target, along with the health care and retail sectors. Indiana-based Matrix Integration and Infotex are partnering to help companies shore up their cybersecurity infrastructure and risk management processes.

STAR Financial Bank is among the institutions that incorporate employee email phishing tests to emphasize the important role of associates in stopping fraud attempts.

not going to tell the news," Shank affirms.

"I bet there's hundreds of breaches that are currently ongoing that no one knows is happening. I don't want to disparage Target, but that (breach) should have been found. If you're not looking for (security gaps), the bad guys are. They're going to burn you."

Anyone can view a list of known ongoing and closed fraud cases on the Indiana Attorney General's web site. *BizVoice*® reached out to some of the companies that have been breached, but none responded to requests for interviews on what they have learned.

Under siege from all sides

Fraud is an umbrella term that covers everything from credit card theft to sophisticated computer hacking. "Big" scores are often the result of social engineering, which includes lottery fraud, romance fraud, impersonation and more; money is rarely recovered and catching or prosecuting fraudsters is difficult.

Shank – who jokes that he got out of law enforcement to "be safe and sit in an office" – had one of the most frightening moments of his career following a case of social engineering fraud.

In late 2016, branch representatives alerted him that an elderly member had been frequently withdrawing unusual amounts of money and acting strangely. When pressed, the member claimed the withdrawals were for a family member in trouble – a flag for potential fraud.

Shank attempted to contact the individual, but was getting no response. He went in person to the member's retirement community to have a conversation about the suspected fraud.

"I said, 'I'm not here to tell you what to do with your money; you can tell me to butt out,' " he recalls.

The member confessed to having won an "international lottery" (those are illegal, Shank reminds) and would be receiving a check for half a million dollars the next day. The member was supposedly sending the taxes and fees to receive the check and was disinclined to discuss the situation because of a confidentiality agreement.

"I'm like, 'You are being scammed. Please don't send them any more money. You will not receive a check tomorrow. When you don't receive that check, please call me back and we can talk further about this. But do not send them any more money,' " he says.

Shank eventually convinced the member not to send more money –$18,000 had already been lost – and later got a phone call from a federal agent linking that member's money to a terrorism group in Thailand. The scary part for Shank is that the member had given Shank's name and his employer's name to the group before deciding it was indeed a scam.

"That's the crazy part. I thought I was putting myself (out of harm's way) and now an Al Qaida group has my name and knows that I stopped them from getting money," he remarks.

Defenders at the ready

Banks have ramped up measures to protect their customers from potential breaches and defend against social engineering and other types of fraud. Most have security or fraud divisions and tools include transaction monitoring.

Consumer buy-in is necessary for those measures to be effective.

Jeremy Vance, security director for STAR Financial Bank in Fort Wayne, explains that transaction monitoring is one of the proactive tools the company uses to detect fraud. Unusual spending patterns will trigger communication from the bank to determine if the purchases are legitimate.

Credit and debit card fraud is frequent, but typically not as costly to the bank. Social engineering is less frequent, but the payout is typically higher for criminals, he says. Authentication methods such as security questions and even biometric identification can help cut down on those instances.

"We want to have good systems and procedures in place to help us identify fraudulent patterns and be able to stop fraud with good authentication methods," Vance acknowledges. "And we want it to be as seamless as possible to the customer."

EMV chip-enabled cards (Europay, Mastercard and Visa) have cut down on credit card fraud by about $10 billion industry-wide, he says.

But that also leads to a resurgence of older types of fraud, such as check fraud.

"They have to find other ways to get the money back out of financial institutions, so it just increases check fraud events. On the digital side, then they think maybe we'll be lax on our old stalwart procedures," he offers. "And as customer convenience increases, the risk of fraud increases as well."

Even chip-enabled technology isn't foolproof. Online purchases, for example, aren't protected by the technology. And some merchants continue to use non-chip point of sale equipment despite compliance rules going into place in 2015. Gas stations have until 2020 for compliance.

If fraud is perpetrated in cases where companies haven't updated their technology, the burden rests on the merchant and not the bank.

"Whoever is operating at the lower level of security is at fault for the fraud. It makes me shake my head where it says, 'Please swipe,' " Shank observes. "Every swipe you can avoid is a chance to avoid (fraud)."

All hands on deck

Kristin Marcuccillli, chief operating officer at STAR Financial, notes that educating and engaging customers is one of the most important steps banks can take to ensure security.

"We conducted surveys of customers and non-customers. … We got a sense of what is most important to them. Fraud protection and identity theft were in the top three," she explains.

Shank urges consumers to take advantage of the various tools Elements offers for fraud protection and identity theft prevention.

"A lot of the regulations that we're under, you have to opt in for a lot of the security protocols, as opposed to them being already on," he allows. "What is the incentive for people to take extra steps to preserve the security of their funds if they don't have a stake in the game?"

Shank and Vance again highlight social engineering – typically perpetrated at financial institutions and other organizations through phishing emails to employees or by impersonating a customer – as one of the major security holes for most companies. Both institutions test their employees frequently with phishing emails to ensure employees are prepared for those types of attacks.

"We send them emails that have a link or an attachment there. We're not trying to make you feel stupid, but this is for preparation. You can't just click on everything that comes in your inbox and assume it's fine," Shank urges.

"I'm of a basic thought that we're all in somebody's hopper. We're in somebody's inbox to have damage done to our identity. We've all been in (cybersecurity data) breaches, we've all had our data compromised. It's just a matter of when the bad guys get around to you in their inbox."

Andy Shank
assistant vice president of fraud investigation manager
Elements Financial

Once more, unto the breach

Two Indiana companies, Matrix Integration and Infotex, teamed up in June to tackle the ongoing security infrastructure needs in the financial industry. Matrix Integration President Nathan Stallings explains how Infotex's focus on information technology (IT) risk management is a natural partner for his technology infrastructure and advisory company.

"One segment with a high degree of need is financial services. (They need) local infrastructure and very secure local infrastructure and data. In working with some of our banking clients, they mentioned Infotex. They come in and check to see how secure it is," he relays.

With better access to information via the internet and online storage and banking, the need for additional security is pressing.

"Some have not even taken basic steps to secure their environment … but the basics will get you 90% there. The extra 10% then becomes not necessarily infrastructure, but training your people on what to do and what not to do," he adds.

Stallings says the operating cost of good security is akin to an insurance policy.

"It's a tough pill for a lot of boards or business owners to swallow, making that cost investment. However, there are too many examples now of where organizations and boards and owners didn't make that critical decision and what it did to their organization."

Knerr, of EY, offers that the benefits to Hoosier companies of utilizing technology far outweigh the risks.

"There is a tremendous amount of productivity and value that companies are getting out of the technology today to run their businesses," he asserts. "There is an ugly side to it. And we adapt to new ways of doing business."

Companies don't need to revert to paper and bury their gold in the backyard. But a top-down culture of security is a must.

"We're hearing the companies that we serve talk about this at the board and at the top level. I think that's very important," adds Christian Bednar, advisory executive director at EY. "When we ask around, are companies viewing this as an IT risk? This is evolving into a business risk and there are cross-functional solutions to help address it. More and more employees and organizations are becoming aware as organizations are evolving their security programs."

Being proactive about security is not just about defending your company; it's about shielding your customers from harm.

"It's money that shouldn't be going somewhere and any money you stop from going to international crime or terrorism is time well spent," Shank concludes. "Good security is good service."

RESOURCES: Andy Shank, Elements Financial, at www.elements.org | William Knerr and Christian Bednar, EY, at www.ey.com | Jeremy Vance and Kristen Marcuccilli, STAR Financial Bank, at www.starfinancial.com | Nathan Stallings, Matrix Integration, at www.matrixintegration.com