WISCONSIN BANKER

AUGUST 2016 | WISCONSIN BANKERS ASSOCIATION | FOUNDED 1892

Tech + Teamwork = Security

Automation and manual systems work in tandem to prevent fraud losses

By Amber Seitz

In 2014, banks suffered nearly $1.9B in total fraud losses, nationally. Criminals use both technology and traditional scam tactics to defraud financial institutions and their customers, so the most effective bank security also leverages the combined power of technology and human discernment to fight back. "You have to layer your security to make it work and function," said **Barry Thompson**, C.R.C.M., managing partner of Thompson Consulting Group, LLC. "Technology is excellent for things like debit card fraud, but some types of fraud require a different layer of security, such as education and training on social engineering." The key is to match the defense tools in your arsenal with the fraud they are best positioned to detect and prevent.

Automation on the Frontline

For some types of fraud, including card fraud and ACH origination fraud, automation can be the best defense. "Automated systems used by most banks detect debit card fraud through patterns of use," said **Joel Williquette**, senior vice president – information security, Bank of Luxemburg. Williquette, also a member of the Federal Reserve's Secure Payments Task Force, explained that many institutions use the automated technology to flag potentially fraudulent transactions and then follow up with a manual review and personal contact with the customer, either utilizing internal staff or third-party vendors.

(continued on p.26)

Responsive By Design

Strategic plans must allow for detours on the road to success

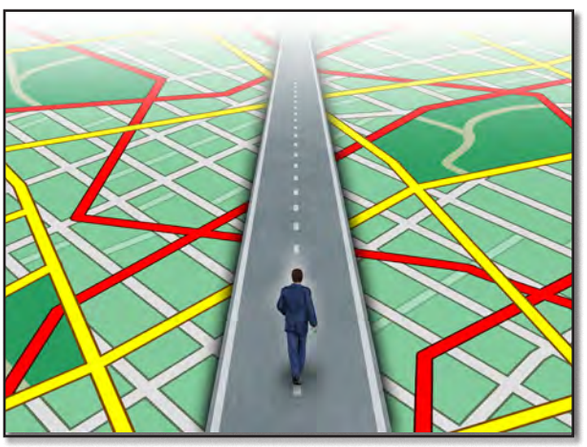
By Amber Seitz

You're on a road trip, and the GPS on your dashboard (or smartphone) assures you that you're following the right path. Then, you hit road construction. You can't follow the path you originally mapped out. What happens? *"Recalculating…"*

Your GPS guides you down a different road that leads you to your intended destination. Your bank's strategic plan should follow the same philosophy: create a plan, but allow for detours. "High-level, when you're looking at the strategic plan and where you're going, you have to be open to modification," said **Marc Gall**, vice president at BOK Financial Institutional Advisors. "The strategic plan is a roadmap, but you need to react to the environment, too."

Plan for Spontaneity

The key to designing flexibility into your strategic plan is to avoid pouring time and effort into creating one, only to have it collect dust on a shelf somewhere. "Get away from thinking of the strategic plan as a standalone item," advised **Ed Depenbrok**, principal at dbrok group, LLC and a director at Ridgestone Bank, Brookfield. "It is a part of how you run the organization." In other words, there must be a connection between the strategic plan and day-to-day activities at the bank. To forge that connection, clearly lay out the specific tactics of how each larger strategic goal will be achieved.



(continued on p.14)

Wisconsin Bankers Association
4721 South Biltmore Lane
Madison, WI 53718

PRSRT STD
U.S. POSTAGE
PAID
UMS

Tech + Teamwork = Security

(continued from p.1)

Debby Bartolerio, assistant vice president compliance and security at Citizens Bank, Mukwonago and 2016-2017 Chair of the WBA Financial Crimes Committee, says they use a similar system (automated software to identify suspicious transactions followed by manual processes) in order to minimize the impact on the customer. "The analysis is done by humans," she said. "In cases where we aren't sure if a transaction is authorized or fraudulent, we would rather allow the transaction and take the chance that it isn't fraud in order to reduce the negative impact on our customers."

Some institutions use automation technology to shift some of the analysis onto the customers themselves, through services such as fraudulent transaction alerts. "It's one of the best services you can give a customer," said Thompson, though he clarified that since these alerts are often dependent on receiving a text message, they are more useful for younger consumers. Going one step further with automation, **Doug Buan**, director – risk management, Wind River Financial recommends incorporating real-time rules into the institution's suspicious transaction software, specifically with card fraud. "Real-time rules will stop payment card fraud transactions from authorizing at the point of sale to prevent loss," he said. "When configured correctly as related to specific fraud situations, this can allow institutions to deploy very effective real time rules while minimizing false positives to legitimate customers."

Blockchain: The Future of Security?

Blockchain, the technology that the digital currency Bitcoin is based on, uses a distributed ledger and encryption for security. However, its potential applications go far beyond digital currency, and some experts predict it will have a significant impact on the financial services industry. In fact, several large institutions are already experimenting with ways to leverage blockchain technology to dramatically increase security and efficiencies in their existing processes. Because it can be used to transfer information as well as currency, blockchain technology has the potential to facilitate more secure tax filings, title transfers and a host of other applications. Like any new technology, blockchain's survival and adoption will depend on a variety of market factors, but banks that choose to ignore it face the risk of falling behind.

Training vs. Social Engineering

With fraud attempted via social engineering, in which criminals attempt to get bank staff to divulge sensitive information, training takes the forefront and technology takes on the role of supplemental tool. "There are so many types of social engineering, it is suggested to combine awareness training and good internal policies to protect our customers," said Williquette. Training and policies are necessary to help mitigate fraud losses due to social engineering, which sometimes occur because the bank staff acted in a spirit of customer service. "One of community banking's strengths is the people. We know who our customers are and what they sound like," said Bartolerio. "The challenge is we have to find employees who are willing to say 'no' when the situation requires it." Training can help mitigate a dangerous, pervasive notion among community bank employees: *That kind of thing doesn't happen here.*

On the policy side, Thompson recommends revisiting the challenge questions the bank uses to confirm a customer's identity. If your current policies list challenge questions such as mother's maiden name, past addresses, or social security numbers, they should be updated. "All of that information can be found on social media websites, and it's not even difficult for most of it," said Thompson. Instead, ask customers for information a social engineer wouldn't readily have access to. For example, if there is no other person on the account, ask

(continued on p.27)

Tech + Teamwork = Security

(continued from p.26)

"What other name is on this account?" because the social engineer will likely offer a guess, rather than specifying that it's not a joint account.

Automation can help flag some of these scenarios, particularly in the case of wire fraud, which saw a sharp spike in 2015, likely due to the escalation of business email compromise (BEC) scams. In BEC scams, the perpetrator mimics a CEO's email and instructs the business's CFO to wire funds. If bank staff don't question the transfer, it can result in significant losses. "Humans can be convinced via social engineering to make exceptions that allow fraud to occur," said Buan. "Automation, correctly configured, can prevent these types of losses from occurring." In the case of BEC scams, the institution could automate a protocol that prevents a wire transfer to a new business until approval from the CEO can be confirmed.

The Top 5 Frauds Attacking Financial Institutions Today:

1. Debit card fraud
2. Email business account fraud
3. Elder fraud
4. Checking fraud
5. Wire fraud

**Based on recent surveys performed by Thompson Consulting Group, LLC*

Structural Defense

Most financial institutions today are organized into separate, siloed departments. While this makes sense for the bank business model in many cases, it is not optimal for preventing fraud. For example, bank staff responsible for electronic funds transfers (EFT) are typically in a back-office department, and have little or no interaction with the IT department. "Your EFT department needs to have a broader understanding of the IT security principles, and the IT department needs a better understanding of the money-moving mechanisms in banking," Williquette explained. "If that cross-pollination isn't happening, it opens up the risk for new types of fraud." To integrate security and fraud prevention enterprise-wide, Thompson advises creating a team that can break down silos and address fraud risk throughout the institution. "You need to have a risk management department or executive risk management committee that can cross all departments," he said. "Banks need to have a risk management system that realizes fraud happens on several different fronts."

No matter how sophisticated the technological tools it uses, fraud prevention ultimately falls on the bank having the right people in the right places with the tools they need to do their jobs. "In the increasingly technological world of fraud, your security or risk management staff cannot help your institution if they are not properly trained," said Buan. "Training and education are important, as well as networking with their industry peers."

Seitz is WBA operations manager – senior writer.

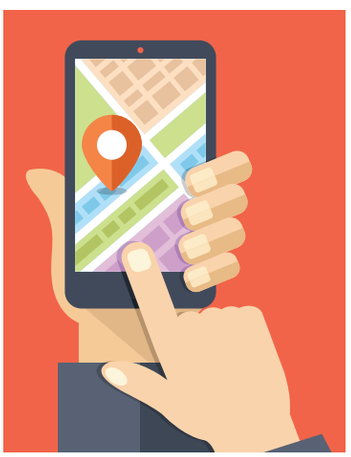
Barry Thompson is one of the expert speakers who will be leading sessions at the upcoming **WBA Secur-I.T. Conference**, held Sept. 20-21 in Wisconsin Dells. His keynote, "Internal Fraud: The Warning Signs" is a can't miss session for bank security personnel, and his breakout session will teach you how to take control of your training and empower your staff to stop fraud losses before they happen. Other speaker sessions include a "Choose Your Own Adventure" live hacking demonstration from Synercomm and a presentation from FBI Special Agent **Byron Franz** on protecting Wisconsin businesses from cyber threats. Visit *www.wisbank.com/Secur-IT* for more information about conference sessions and to register!

Want More Information about Security and Fraud Prevention?

Banks Weighing Their Options, Opportunities for Augmented Reality Games

By now, you've probably heard a lot about the augmented reality mobile game "Pokémon Go," released in early July. The goal of the game is to collect (or "capture") digital creatures called Pokémon by traveling to real-world locations. At some of these locations, called Pokéstops, players can compete with one another or buy items to advance their game. Some financial institutions quickly identified this as a marketing opportunity and began advertising their proximity to Pokéstops or PokéGyms, and some even purchased lures to bring in more Pokémon (and therefore more foot traffic).

However, banks also need to consider the potential security risks of embracing the "Pokémon Go" craze. For example, since players must view the world around them through the camera on their smartphone when searching for Pokémon, banks may need to create policies or procedures to respond to individuals who come into a branch and start exploring.



To help mitigate some of these risks, WBA issued a press release on July 14 to help educate consumers and advise the use of caution and common sense when playing in or near a financial institution. If you wish to remove (or add) your bank's location as a Pokéstop, detailed instructions for submitting the request to the game developer can be found here: *www.techrepublic.com/article/how-to-remove-your-business-location-from-pokemon-go/*. You can read the WBA press release at *www.wisbank.com/PressReleases*.