As fraud incidences rise, so should banker vigilance

By Jackie Hilgert

Protecting a bank from the ubiquitous data breach involves training, the right levels of insurance coverage, and a close attention to vendor contracts. That was the message delivered by Kris St. Martin, vice president and Bank Program Director of CBIZ, and Carolyn Purwin Ryan, a partner in the law firm Mullen Coughlin, during an Oct. 8 breakout session at the BHCA Fall Seminar.

Trying to mesh customer convenience with security is increasingly difficult. Artificial intelligence, deep fakes, and social engineering fraud have grown sophisticated. At the root of social engineering fraud is a takeover and subsequent monitoring of an email account.

St. Martin laid out the details of a social engineering fraud he worked through that led to wire fraud. The issue stemmed from the sale of a farm worth approximately $8 million. The owners were represented by a realtor whose email had been compromised. As a result, fraudsters knew all of the details of the closing and sent false wiring instructions. Fortunately, the fraud was detected before the money vanished from the bank that received the wired funds. "Even if this was not the bank's legal liability," St. Martin explained, "the pain and the amount of time that the bank would have to deal with this, what customers would be going through, would just be immense."

St. Martin said banks are upping their training for staff and for customers. "They're doing seminars; they're doing webinars; they are talking to their customers about all these kinds of fraud," he said. "The more I think you educate your customers on all of this, it's going to create goodwill to your customer, reduce their potential liability."

St. Martin said he frequently works with groups of bankers to deconstruct attacks to help train teams how to spot attacks, and how to respond. "I'm a big proponent in educating your customers in any fashion possible," St. Martin said. "It helps create goodwill. It helps them stay out of trouble. And, it's a little bit harder to sue somebody who you think has been a good advocate."

Also wise is reviewing bank policies for wire transfers with customers. "Banks must be able to defend their wire transfer process," St. Martin said. "I think that's good practice anyway."

It's also important to review insurance coverages with an agent/carrier. "A lot of people assume [wire fraud] is part of your cyber policy," St. Martin said. "It's not; it's part of your crime bond policy because it's theft of money. That's where you've got to look at the different scenarios and make sure you have the right coverage of the bond itself."



Carolyn Purwin Ryan of the Mullen Coughlin law firm, and Kris St. Martin, CBIZ

Some of the greatest headline generating breaches of 2024 occurred outside of banking, but could well have impacted banks. This opened the door to discussing how vendor relationships create vulnerabilities, especially when a vendor has access to a bank's data (think core provider).

Before something like this occurs, Purwin Ryan said, find out what the vendors' obligations to the bank are. They might limit their obligation to simply notifying banks which customers are affected, placing the onus to notify on the bank, she said, encouraging bankers to look at vendor contracts before a breach occurs to see where the limitations exist. Most contracts, she said, are written to benefit the software companies. "It is important to take a look at those contracts to determine who is the data owner ... because that ultimately decides who is going to be going through the notification process." She also suggested a timeframe for notifications be laid out in the contract.

Be wary also of language that limits vendor liability to what you are contracted to pay them for a certain term. If you are contracted to pay $50,000 in one year for their service for example, St. Martin said, the ceiling for their liability might well be $50,000. "In a lot of these fraud cases, that isn't nearly enough," he said, especially if the bank is later sued as a result of the breach.

Compared to other business sectors, banking has led in the prevention of cyber fraud, St. Martin said. Yet technology is allowing bad actors to continue to gain an edge. And it's working. A study conducted by the Federal Reserve Bank of Boston indicates that check fraud in 2023 was $20 billion, up from $100 million in 2006.

The imperative, therefore, is to stay vigilant, urged St. Martin: "Question the experts within your bank and ask good questions, like: "How do we handle these types of things?" ■