Oklahoma Bankers Association marks increase in check, wire fraud attempts

Oklahoma Bankers Association recently issued a Fraud Alert, a notice seldom sent to its members. The notice brings to light increases in two types of fraud at banks: Check fraud and wire fraud.

Regarding check fraud attempts, banks have reported receiving "account funds availability" verification calls on existing accounts, followed by a call from the "customer" who claims to be sending someone to the bank to cash a large check.

OBA said that the surge in check fraud is due to "social engineering," defined as using deception to manipulate individuals into divulging confidential or personal information. They added that recent fraud attempts have been valued in the tens of thousands of dollars.

"This is a regular issue we're seeing, and I would be most apprehensive about social engineering," said Don Pape, an Of Counsel Attorney at Phillips Murrah who specializes in banking law. "There are people who will, in essence, test the security of large companies and will manage to move into the company. Employees need to be cautious when receiving requests from people they don't know well, and be diligent when verifying wire transfer requests."

OBA suggests banks consider having a manager involved in the process of dispensing large amounts of cash. Managers should follow up calls from the alleged "customer" with a call to the

customer number on file. This procedure is similar to that of wire fraud protection procedures, they said.

Hackers are watching

A surge of wire fraud activity has also been linked to social engineering, whereas cyber criminals hack into business emails for extended periods of time and mimic emails requesting wire transfers within a company. They are able to seem more authentic by replicating language patterns and having knowledge of a customer's daily activities.

"The problem comes in when banks call back a customer to verify a transfer and 'Partner A' confirms based on what 'Partner B' says without realizing 'Partner B' was actually the person hacking the account and making the fraudulent request," said Elaine Dodd, Executive Vice President of OBA's Fraud Division. "Hackers previously observed email activity for 229 days. We've seen an increase to 300 days for hackers to gather information about a victim's family or daily appointments in order to send fraudulent emails at the most opportune time, likely when the victim is off work or on vacation."

There is an increased amount of information fraudsters have on customers, and this is contributed to any number of recent massive data breaches, Dodd said.

"Really scrutinize where a wire fund request email comes from," she advised. "If something feels wrong, little details can clarify a source."

For example, she recommended that the recipient should closely check the sender's email address to be sure it's authentic.

"Usually, the change is nothing substantial, perhaps a period or letter," She added. "The best thing to do to be safe is pick up the phone and call the person requesting wire."

OBA provides retail training on this topic to help bankers better inform and protect customers.

“Stay safe out there,” Dodd said. “I encourage anyone who has working knowledge of these types of frauds to share in their social circle, business and social. We could all be at risk.”