Need Assistance?
bigimarkets@iiaba.net
703-647-7800 (9am-5pm ET)

Helping Banks Help Themselves

One increasing claim trend seen at Travelers among financial institutions is a form of social engineering referred to as fraudulent instructions. In a bank's case, fraudulent instruction occurs when an employee is tricked into transferring money from a customer's account to somewhere else because a fraudster steals the customer's identity and convinces the bank through emails or phone calls to move the funds. With the benefit of seeing multiple claim scenarios, Travelers would like to share some of the best practices that can be used to prevent fraudsters from making your bank a victim.

- Train your staff. The Number 1 way to prevent fraudulent instructions is to have a well-trained staff that follows procedures, verifies a customer's instructions by calling the customer at a pre-determined number, and questions things when they don't look right. Your staff should not only understand the procedures but also why they are important. Train your staff not to deviate from procedures by taking shortcuts.
- Deliver good customer service, but make the customer prove who they are. Don't hand the customer answers. In a recorded call, a bank employee was trying very hard to give the member excellent customer service but did so at the expense of the real customer. To questions such as "Are you still at 123 Main Street?" and "Is your phone number still 555-5555?" the crook simply had to acknowledge that the information was correct. Staff should require the customer to authenticate their personally identifiable information rather than acknowledge what is on file.
- Know your customer. If a bank employee thinks a wire request is unusual for a certain customer, they should be empowered to dig further. Travelers had one claim where an 80-year-old customer requested a $750,000 draw from his home equity line of credit to be wired to Australia. When asked what the transfer was for, the purported customer said he was buying a rock quarry. Unusual requests should spark increased due diligence.
- Escalate suspicion. Train your people that if they get a call that sounds suspicious, they should share it with others on the team. Just because one customer service representative wouldn't complete a transaction doesn't mean another attempt won't be made. It is important to talk amongst yourselves. These fraudsters are diligent, so bank employees must be, too. A consistent pattern exists: Crooks don't stop at just one attempt. They will keep calling back until they either get caught or there is no more money.
- If a customer says they can't be reached at the phone number on file, call it anyway.
- Beware of urgency, poor grammar, the word "kindly," and sentences that don't make sense or use improper words.

When these steps are taken and a socially engineered fraudulent instruction attempt fails, celebrate that success. If an employee prevents a fraudulent transaction, spread the news. Share the emailed instructions, discuss what was suspicious about it and post examples of fraudulent instructions. This helps the front-line team remember that attempts at fraudulent transactions are real and are constant. Bank employees must remain vigilant.

Travelers SelectOne® for Community Banks, underwritten by Travelers Casualty and Surety Company of America, is endorsed by the Independent Community Bankers of America. To find your local community bank, visit ICBA's community bank locator at www.icba.org/about/find-a-community-bank. Simply type in your zip code and the app will show you all the community banks in your area. A specimen policy is located in "Product Resources" on www.bigimarkets.com.

Original Article Publication Date November 12, 2019

Travelers is committed to managing and mitigating risks and exposures, and does so backed by financial stability and a dedicated team - from underwriters to claim professionals - whose mission is to insure and protect a company's assets.

Original Article Publication Date November 12, 2019