Protect Your Bank from being a Victim of Fraud

Social engineering scams, such as fraudulent instruction, continue to affect consumers and businesses alike. 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 has stolen the customer's identity and convinced the bank through emails or phone calls to move the funds. By following the best practices below, you can help prevent fraudsters from making your bank a victim.

- **Train your staff.** The No. 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 understand not only 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 customers prove who they are.** Don't hand the customer answers. In a recorded call we listened to, a bank employee was trying very hard to give the customer 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 customers 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. We 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 staff to share suspicious calls 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 among 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 either they get caught or there is no more money.
- **Make the call.** If a customer says they can't be reached at the phone number on file, call it anyway.
- **Be suspicious of bad grammar.** Beware of urgency, poor grammar**,** the word "kindly," and sentences that don't make sense or use improper words.

If an employee prevents a fraudulent transaction from occurring, spread the news and celebrate that success. Share the fraudster's emailed instructions, discuss what was suspicious about them and post examples of other fraudulent instructions. This helps front-line team members remember that attempts to use social engineering tactics to generate fraudulent transactions are real and constant. Bank employees must remain vigilant.

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. For more information, visit www.travelers.com or talk to your independent insurance agent about social engineering coverage.