intact financial services

NEWS FROM THE VAULT

November 2021 | Issue 28

How your customers are becoming victims of wire fraud

BY CRAIG M. COLLINS – PRESIDENT, FINANCIAL SERVICES

Incidents continue to be reported to banks and their insurers involving data compromises that occur at the bank customer's location. This article will provide some of the most common and evolving methods of data compromise.

Banks are saddled with a dual duty when it comes to wire transfers – securing against wire fraud through your own policies and procedures, and helping your customers secure themselves against data compromise. Fraudsters are accessing customer information from hacked emails or websites, stolen checks, and public filings; and from the customers themselves through deceit or false pretenses, like calling and claiming to be someone from the bank. The first step in helping your customers is to ensure they are aware of the most common ways their data can be compromised.

1. This is your banker calling…

- Through fake or scam phone calls, someone claims to be calling from the bank and asks the customer for their banking information. If the information is provided, the fraudster sets up online banking for the customer's account, without their knowledge and causes funds to be transferred via the online banking platform.

2. They know everything about you…

- Familiar with data scraping? Data scraping is the process of extracting data from a website or social media platform using automated tools. This process enables the collection of vast amounts of publicly available information. Scammers can catalog and aggregate data to create enormous datasets, which they sell to cyber criminals who use them to create personal or professional profiles of individuals. This information can be used in a variety of ways to trick your customers into revealing their private banking information.

3. Your email has been compromised…

- Fraudster monitors customer's email traffic and presumably gathers necessary information from valid emails and other public sources (i.e., public mortgage records); then poses as the customer and sends emails to the bank requesting additional wire transfers. Typically, the customer is unaware this is happening.
- In some situations, a fraudster hacks a customer's email, or the email of someone outside the bank with whom the customer has business dealings with. They gather the necessary information and intercepts an email from the other party to the customer with wire transfer instructions that are fraudulent.

4. If it sounds too good to be true…

- A “too good to be true” job is posted online. The applicant is hired sight unseen, and the “employer” offers to pay you upfront, asks to accept deliveries or make purchases on their behalf. The employer sends a bad check to be deposited in the applicant’s personal bank account which ultimately bounces, and their account is emptied.

It’s important to arm your customers with ways to protect themselves. Remind your customers often of the following helpful tips:

- Never give out your bank account information to anyone – in person, over the telephone, email, etc.
- When signing up for social media accounts, creating profiles, and posting details about your personal or professional life, provide the bare minimum of information.
- Minimize the risk of your emails being compromised – don’t click on links in emails (open a browser and type the website address) and always look at the sender’s email address to make sure the domain is accurate. If your email is compromised, notify your bank immediately.
- Check your accounts online frequently, or even daily, for fraudulent transactions or activity.
- It’s imperative that the customer verify wiring instructions they receive from a third party before forwarding them to the bank.
- Don’t cash or deposit checks from any potential employers and then send money on or wire it back.
- Don’t accept payments from anyone you don’t know or have never met.
- Confirm privacy setting on all personal devices and online services.