ACH and Wire Transfer Fraud Prevention Tips

ACH (automated clearinghouse) transactions and wire transfers are two forms of electronic funds transfers (EFTs) and the fastest ways to send cash to another business, individual, or other recipient.

Businesses are a target in which cyber-criminals employ phishing emails, compromised websites, malware, and other tools to steal bank login credentials, then transfer money out of the victim's bank account and into the thieves' account—often, at a bank halfway around the world, where the funds cannot be recovered. Criminals target small-to-medium-sized businesses because they are less likely to have the strongest information security safeguards.

To better protect your business, consider implementing the following best practices:

- Verify changes in vendor payment location and confirm requests for transfer of funds by phone. Never initiate any changes based only on email communication.
- Be wary of free, web-based email accounts, which are more susceptible to being hacked.
- Be careful when posting financial and personnel information to social media and company websites.
- Regarding wire transfer payments, be suspicious of requests for secrecy or pressure to take action quickly.
- Consider financial security procedures that include a two-step verification process for ACH & wire transfer payments.
- Create intrusion detection system rules that flag emails with extensions that are similar to company email but not exactly the same. For example, .co instead of .com.
- If possible, register all Internet domains that are slightly different from the actual company domain.
- Know the habits of your customers, including the reason, detail, and amount of payments. Beware of any significant changes.