VALUABLE INFORMATION TO PROTECT YOUR VALUABLE INFORMATION

HOW IS IT DONE?

Fraud through ACH and wire transfers is fairly simple considering all perpetrators need is an account number and bank routing number. ACI Worldwide, a Universal Payments Company, recently published an article discussing the following methods perpetrators use to commit ACH and wire transfer fraud:

- **Account takeover:** The account takeover occurs when the fraudster opens a fake business account with Bank A. The perpetrator then targets account holders at Bank B through phishing attacks, which could include an email with a link, taking them to a bogus site where they enter their login information, which the fraudster captures. Now that they have the account holder's information, the fraudster accesses Bank B's customers' bank account online. They then initiate an ACH to the fake account at Bank A. Once the funds have been transferred to Bank A, the fraudster initiates a wire transfer from the fake account to another account that they control and sweep the money away.

- **Man in the middle attack:** This attack involves malicious code, hidden in an email scam, link to greeting card, or news story which infects the account holders' computer with a virus that collects data typed into Web forms. Once the banking information is collected, the fraudster utilizes a scam to target the specific bank account, sending the account holder to a page to reset their security code, which installs another virus. The next time the account holder logs into their online banking account, the fraudster's virus inserts itself between them and their online banking system, where it executes commands to initiate wire transfers or ACH transactions without the knowledge of the account holder.

- **Social engineering attack:** Fraudsters use psychological manipulation to trick people into divulging account information. This can be done by someone calling a business employee, claiming to be an IT employee, to gain access to his or her computer on which the fraudster could install spyware or keystroke loggers.