What is CATO?

Corporate account takeover is a type of fraud where thieves gain access to a business' finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable.

Attack Types

- Hacking
- Virus
- Phishing/Spear Phishing
- Social Media

How do you prevent CATO?

- **Educate your employees**. You and your employees are the first line of defense against corporate account takeover. A strong security program paired with employee education about the warning signs, safe practices, and responses to a suspected takeover are essential to protecting your company and customers.
- **Protect your online environment.** It is important to protect your cyber environment just as you would your cash and physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated virus protections on your computer. Use complex passwords and change them periodically. Keep your computer, antivirus, and programs up-to-date.
- **Partner with your bank to prevent unauthorized transactions**. Talk to your banker about programs that safeguard you from unauthorized transactions. Positive Pay and other services offer call backs, device authentication, multi-person approval processes and batch limits help protect you from fraud.
- **Pay attention to suspicious activity and react quickly.** Look out for unexplained account or network activity, pop ups, and suspicious emails. If detected, immediately contact your financial institution, stop all online activity and remove any systems that may have been compromised. Keep records of what happened.