PROFILE BANK
Your Neighbor. Your Partner. Your Bank.

Commercial Services Security Newsletter

June 2023 | CSN - Q2 - 2023

FS-ISAC

Current Fraud Risks and Prevention Tips

Has your business been a victim of fraud? The Consumer Sentinel Network received 2.4 million fraud reports in 2022, down from 2.9 million in 2021; however, almost $8.8 billion in total reported losses in 2022 surpasses the $6.1 billion figure from 2021.

The skill level and diversity amongst fraudsters means that small and medium sized businesses are required to pay more time observing, tracking, and monitoring these financial crime types:

- Automated Clearing House (ACH) and wire transfers
- Business email compromise
- Checks
- Credit and debit cards
- Fake invoices
- Online purchases
- Ransomware

Fraudster Tactics

Knowing the basic tactics commonly used by fraudsters will help your employees be on the lookout when something suspicious is happening.

1. **Scammers pretend to be someone you trust.** They make themselves seem believable by pretending to be connected with a company or a government agency you know.
2. **Scammers create a sense of urgency.** They rush you into making a quick decision before you look into it.
3. **Scammers use intimidation and fear.** They tell you that something terrible is about to happen to get you to send a payment before you have a chance to check out their claims.
4. **Scammers use untraceable payment methods.** They often want payment through wire transfers, reloadable cards, or gift cards that are nearly impossible to reverse or track.

Reducing Your Risk

Regardless of the fraud risks, providing consistent training for all of your employees can reduce your fraud exposure. Invest in fraud prevention products. Adhere to PCI standards to protect stored data.

Fraud Type	Characteristics
 Altered, either as to the payee or the amount Counterfeit Forged, either as to signature or endorsement Drawn on closed accounts	The check shows signs of tampering Images and text are not crisp and professionally produced There are misspellings or poor grammar on the check If paying by mail, the return address on the envelope may be different than the check address Magnetic Ink Character Recognition (MICR) encoding at the bottom of the check does not match the check number
 Business email compromise Executive email compromise Fraudulent payment for products	Internal executive request to transfer large sum of money Emailed transaction instructions containing different language, timing, and amounts than previously verified, authentic transaction instructions Wire transfer goes to a foreign bank
 Credit and debit cards Online purchases	Large order(s) in high quantity along with different card numbers Big ticket purchases and international shipping Multiple orders using similar card numbers except for the last four digits Suspicious credit card with bank ID numbers that do not belong to the bank One card purchase using multiple shipping addresses Purchases using different cards with the same address
 Fraudulent billing invoices for non-existent products and services	Duplicate invoices Legitimate invoices with inflated charges Invoice for supplies that were never received or needed

