

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.

Did You Know?

- ▶ Commercial Bank offers fraud prevention tools to help you manage fraud activity.
- ▶ *Positive Pay* can enable you to:
 1. Reduce your potential exposure to check fraud
 2. Quickly identify suspicious items
 3. Have ready access to check images
- ▶ *ACH Blocks and filters* can:
 - Block specific companies at an account level
 - Allow only pre-authorized companies, creating exceptions for all other transactions
 - Filter transactions based on designated amount

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 like ACH blocks and filters, and positive pay. Adhere to PCI standards to protect stored data.

Fraud Type	Characteristics
 <ul style="list-style-type: none"> ▶ Altered, either as to the payee or the amount ▶ Counterfeit ▶ Forged, either as to signature or endorsement ▶ Drawn on closed accounts. 	<ul style="list-style-type: none"> ▶ 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
 <ul style="list-style-type: none"> ▶ Business email compromise ▶ Executive email compromise ▶ Fraudulent payment for products 	<ul style="list-style-type: none"> ▶ 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
 <ul style="list-style-type: none"> ▶ Credit and debit cards ▶ Online purchases 	<ul style="list-style-type: none"> ▶ 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
 <ul style="list-style-type: none"> ▶ Fraudulent billing invoices for non-existent products and services 	<ul style="list-style-type: none"> ▶ Duplicate invoices ▶ Legitimate invoices with inflated charges ▶ Invoice for supplies that were never received or needed