2022 Edition

# Commercial Fraud Prevention Guide

A simple and easy guide to help you keep your business safe.

*business* banking for good

# Fraud Types

**Recognizing the different types of fraud can leave you better equipped to prevent it from happening.**

## Check Fraud

Check fraud is a rampant and serious issue. Be sure to examine the check for changes to the payee name, dollar amount, and signs that the check has been "washed". A best practice to protect your account information is when mailing checks, always use a secure drop off location such as the USPS mailbox. Daily monitoring of checks through the account is recommended to ensure checks have not been altered.

## Account Takeover

Corporate account takeover is a type of fraud where an unauthorized third party gains access to a business's finances. This can include taking over an online banking profile or accessing payroll systems. Many times the funds that are sent are unrecoverable. A best practice is to ensure your anti-virus and malware are up-to-date on your computer. Also, ensure that dual approval capabilities are in place to verify transactions by more than one person.[1]

## Impostor Fraud

Fraudsters can create or manipulate contact information and act as individuals you know and trust to appear legitimate. This allows the fraudster to request payments or change payment instructions such as invoices or payroll information, and can include changes to the type of payment such as ACH to wire. This can be accomplished through email compromise, phone calls, or text messaging. A best practice is to never accept payment instructions in the form of an email without verbal verification. The best safe guard when accepting payment instructions is to request they be made in person whenever possible. If a payment must be received by email, never accept payment instructions without completing a verbal verification.

[1] "Protect Your Small Biz Account." ABA. Accessed October 26, 2022. https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/protecting-small-biz-accounts

# Fraud Types (Continued)

## Business Email Compromise (BEC)

A business email compromise is a sophisticated online crime where criminals gain access to company networks using malware or spoofing an email account or website. The impostor will then send email messages that appear to come from a known source making a legitimate request often in regards to billing, invoices, title, and real estate. The information that is gained is used to send a request using an email address that may have slight variations from what the legitimate email address is. The compromised email is then used to send a notification to update payment information. Once the payment is processed the funds are then sent to the scammer.

To protect yourself against BEC make sure to verify payment and purchase requests in person if possible or by calling the person to verify information at a known phone number, not included in the email correspondence. Impostors hope to outsmart you when you receive the payment instructions in the email; they are anticipating that you do not verify the updated payment instructions verbally. Do not click on any links in an unsolicited email or text message. Be sure to carefully examine the email address, URL, and spelling used in the correspondence. Be cautious of what you download and any email attachments that are forwarded to you. If the requester is pressuring you to act quickly, slow down and reverify the situation and the information.

### At a glance...

**71%** of organizations were victims of payment scams.[2]

**68%** of companies were targeted by Business Email Compromise (BEC).[2]

**66%** of payment methods impacted by fraud activity were checks.[2]

[2] "2022 AFP Payments Fraud and Control Survey" APF. Accessed October 26, 2022. https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

# Fraud Prevention

**There are many actions you can take to reduce the likelihood of fraud. Here's how you can get started.**

## FirstBank Tools

### Alerts

Setting up Alerts through your online services will allow for improved monitoring of your account activity.

### Positive Pay Service

The Positive Pay Service offers quick detection of fraudulent checks that are presented against account(s), allowing you to return them prior to final payment.[3]

## Operational Controls

### Self-Evaluation

Perform monthly, quarterly, semi-annual, and annual reviews on internal users and their account activity. Educate employees on best practices for fraud prevention.

### Internal Controls

Create processes to ensure that all requests are valid and verified. If you need assistance in crafting tailored solutions within Internet Cash Management, our Treasury Management Specialists are available to help.

### Device Security

Look carefully make sure the devices you use for banking are secure and regularly updated.

[3] Please note Positive Pay is only available to clients who utilize Internet Cash Management.

# FirstBank Resources

**We're here to help! Below are a few of our fraud prevention solutions that can help your business.**

## Treasury Management Department

Available Monday–Friday, 7:30am–5:30pm. The Treasury Management Department can be reached at 303.235.1378 or 855.426.1500, option 5.

## 24-Hour Department

Outside of regular business hours, our 24-Hour department can be reached at 303.237.5000 or 800.964.3444.

## Annual Security Forum

FirstBank holds a security forum each year to address trends and fraud prevention. Contact us at 855.426.1500, option 5 to learn more.

## Branch Contact

For additional questions, please visit any of our locations. To find a branch near you, visit us at efirstbank.com/locations.

# Thank You

*business* banking for good


Member FDIC