BUSINESS FRAUD

First Bank & Trust

What to Do When Fraud Happens

As soon as you suspect fraud, move quickly to limit the financial damage.

1. **Secure financial accounts:** Contact your financial institution and change your log-in credentials.
2. **Report the fraud:** Your financial institution can assist in reporting the incident to law enforcement, FTC, IC3.gov, and others.
3. **Monitor and recover:** Once the fraud incident is secure and under control, review current business practices to ensure the risk of future events is mitigated.

If you suspect a call, email, or text claiming to be from First Bank & Trust is fraudulent, do not provide any information. Instead, call us immediately at our toll-free number: 800.843.1552.

Common Business Fraud

Business Email Compromise

Business email is taken over, and an email is sent appearing to be legitimate. Payment details and/or account information will be requested to be changed, and then an urgent payment will need to be sent.

Check Fraud

The deposit account number is compromised and then used to create fake checks with the business account number. Checks are stolen from mailboxes, altered, and processed.

CEO Fraud

Criminals will target executives in the business. The high-level employee will then appear to be requesting that payments be sent, and due to their level of seniority, other employees do not question the request and instead act.

Social Engineering

Numerous methods are used to trick employees into giving control over their devices or sharing information that can later be used to commit fraud against the business.

Payroll Diversion

Human resources receives an email from an email address that is compromised. Criminals request updates to direct deposit or payment information, causing future payroll to be sent to a fraudulent account.

Best Practices to Prevent Fraud

- **Discuss fraud and scam red flags** regularly during meetings, and train employees consistently to recognize and respond to potential threats.
- **Implement strict procedures** for verbal verification of all payments, invoices, and account changes. Verify each transaction verbally, and establish an urgent response process for addressing any discrepancies.
- **Enforce the separation of duties** to help identify fraud earlier. Ensure no single employee is responsible for all transactions and reconciliations.
- **Utilize check and ACH positive pay**, if available, through your financial institution.
- **Use digital banking to review account activity daily**; monitor transactions promptly, ideally each day, to enable quick reporting to your financial institution and maximize recovery opportunities in case of fraud.
- **Review fraud controls** with all vendors that are active in your business.
- **Secure account numbers**, EINs, and any other sensitive identifiers that could be used to commit financial fraud against the business.
- **Have an IT cybersecurity expert** available to consult when the need arises.
- **Minimize the amount of paper** your business uses. Any paper trail of account information provides a risk.
- **Move to digital payment options** when available. Minimize use of paper checks.

More Fraud Resources for Businesses