Fraud Awareness and Prevention Checklist

Safeguards no business should be without.

No business is 100% safe from fraud, but you can take steps to minimize the chances of it affecting your business. Protect your accounts, identity, and financial well-being from the malicious actions of scammers by using these best practices.

What is Fraud?

Fraud can occur when someone uses your account to make unauthorized purchases or transfers. This can happen if another person obtains your credit or debit card, card number, online credentials, or other account details.

Watch for the Red Flags of Fraud

Criminals are adept at making fraudulent communications appear to be from legitimate sources to induce individuals to reveal personal information. Whenever you get a message that seems like it is from a financial institution, do this:

- **Stop:** Resist immediate action when receiving an email, phone call, text, or person-to-person payment request.
- **Look:** Check for anything unusual about the message, like typos, unknown URLs, attachments, scare tactics, threats, or high-pressure language.
- **Think:** Be skeptical. The safest choice is to end communication and contact your bank directly.

Transaction Controls

- Review and reconcile accounts daily and monthly.
- Secure check stock and manage under dual control.
- Never sign blank checks in advance of payments.
- Secure file access (including trash bins) from non-employees.
- Bank online from a separate computer with no access to email or web surfing.
- Use free electronic statements to prevent information from being stolen from the mail.
- Use direct deposit and electronic bill-pay to prevent checks from being stolen in the mail.

Internal Controls

- Enable multifactor authentication (MFA) to protect your account from unauthorized access. Sometimes called "Two-Step Verification," MFA is a way of confirming your identity when you try to sign in.
- Use dual control for all monetary transactions, including ACH originations, wire transfers, and bill pay.
- Set policies for password security and never reuse passwords.
- Update antivirus software regularly and set it to run automatically.
- Install a firewall as a first line of defense against hackers. Never leave a computer unattended while logged into online banking.
- Never use online banking in public spaces with unsecured Internet access.

Report Suspicious Activity

First Interstate Bank has a policy of **NEVER** reaching out to clients by email, text, or phone call and asking for personal financial information such as account numbers, balances, PINs, or debit/credit card numbers. Please report suspicious emails, text messages, phone calls, or websites that claim to be from First Interstate Bank.

- To report debit card fraud, call **833-699-0076**. For credit card fraud, call **866-839-3485**. To report all other fraud, contact your local branch during business hours.
- Report suspicious emails, websites, or text messages that claim to be from First Interstate Bank to **phishing@fib.com**

LEARN MORE

Follow **#BanksNeverAskThat** on social media for quick tips, or speak with your trusted banking representative about steps you can take to protect your accounts.

First Interstate Bank®
Built for you.

firstinterstate.com

Member FDIC. Equal Housing Lender.

OS_03/18/2024