FIRST BANK

Defeat the Fraudsters:

Checklist to help protect you against account fraud

Account takeover fraud is a form of identity theft where a fraudster gains access to a victim's accounts and personal information. They can then use the information to perform a number of different fraudulent acts, including transferring funds, modifying personal information, and adding other "authorized" users. Combating this type of fraud requires understanding and action steps to make sure your business or organization is not at risk.

Use this checklist to help ensure you are decreasing your risk of account fraud.

☐ **Protect your information**

Be cautious if someone is asking you to share personal information that may provide access to accounts. First Bank will never ask you for your Secure Access Code over the phone, through text, or email.

☐ **Create strong and unique passwords**

The use of numbers, capital letters, and special characters can help strengthen your password. Also consider updating passwords periodically.

☐ **Set up multi-factor authentication**

Adding a second step of verification to your network and accounts makes it harder for others to access your information. This can be as simple as receiving a code via text or email, or installing a third-party authentication app.

☐ **Require dual approval**

Utilize dual approval methods on ACH and wires by notifying an approver that a file is ready.

☐ **Virus protection on all technology**

Don't forget to include phones and tablets when adding virus protection on computer systems.

☐ **Disable call forwarding with your cell phone provider**

Fraudsters are social engineering cell phone carriers to forward phone calls and text messages to intercept valid calls, messages, and conduct fraudulent activity.

FIRST BANK

☐ **Have a payroll system in place**

Implement a payroll system, so employees aren't tempted to provide information via fake payroll platforms that spoof employer data.

☐ **Verbal verification process**

Call back your vendors and employees when changes to account information are sent via email or fax.

☐ **Never click on links from unknown senders**

Links and attachments are an easy way for hackers to get private business information. Always verify that you know who it is sending or requesting information. Our series, The Adventures of Amelia N. Bochs, teaches you what to look for to avoid potential hacking attempts. Learn how to protect yourself: The Adventures of Amelia N Bochs Series

☐ **Update your web browser**

Ensure you are using the most up-to-date web browser to prevent cybercrime and data hacking. First Bank has a variety of resources available on fraud prevention and identity protection. View articles on the Learn section of our website or start our free course: Identity Protection.

☐ **Consider a fraud detection tool**

Our Positive Pay tool identifies unauthorized transactions before final payment, so you can feel more secure about the money coming out of your accounts.

☐ **Sign up for alerts & text banking**

Receive First Bank alerts on deposits, transfers, payments, and more. Text banking allows you to receive information about your accounts instantly.

Contact the First Bank **Business Support** team to learn more about what First Bank can do to keep your business protected.

Suspect fraud? Give us a call immediately!
Business Support: (866) 435-7208