Business Online Fraud Prevention

With the increase in cybersecurity threats, we would like to update you on some ways to protect yourself against fraud when you're using Business Online Banking.

SecurID Tokens

At Lake City Bank, companies that originate wire transfers or ACH transactions via Business Online must use a SecurID token to login and release transactions. In addition, a second user also must login with a SecurID token to authorize transactions. This dual authentication and approval process helps eliminate opportunity for fraudsters to send unauthorized payments.

Out of Band Authentication (OoBA)

Lake City Bank also has invested in Out of Band Authentication (OoBA), which authenticates the user at login. OoBA recognizes when users log in to a service from a device (computer, laptop, mobile device, tablet, etc.) that is different from their normal routine. OoBA verifies factors such as IP address, computer ID, etc. and checks them against normal activity for specific users. If something is out of the ordinary, users are prompted to receive a unique code by text or phone to a pre-specified number.

Set Up Business Online Alerts

Lake City Bank recommends activating the following alerts.

ACH Template Activity – Notifies you when an ACH template has been added, edited or deleted.

Outgoing Wire Status Change – Notifies you when an outgoing wire's status changes from the selected account.

Wire Transfer Template Activity – Notifies you when a wire transfer template has been added, edited or deleted.

Positive Pay and ACH Positive Pay alerts – Alerts you when someone is trying to present unauthorized checks or ACH debits to your account.

To set up these and other account alerts in Business Online, go to the Administration tab and select Manage Alerts under the Communications heading. For more information about managing alerts, see page 10 of Lake City Bank's Business Online User Manual (lakecitybank.com/bizmanual).

Avoid Phishing, Spyware and Malware

- Don't open email from unknown sources. Be suspicious of emails claiming to be from a financial institution, government agency or other organization requesting account information, account verification or banking access credentials such as usernames, passwords, PINs or similar information. Lake City Bank will never ask you for this information.
- Never respond to a suspicious email, click on a link or open a file attachment embedded in a suspicious email, which can expose your system to malicious code that could hijack your computer. Call the source on a known number if you are unsure who sent an email.
- If an email claiming to be from Lake City Bank seems suspicious, check with us to confirm it is legitimate.
- Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.

Lake City Bank

- Update all of your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.
- Ensure computers are patched regularly, particularly your operating systems and key applications.
- Install a dedicated, actively managed firewall, especially if you use a broadband or dedicated connection to the internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers.
- Check your settings and select at least a medium level of security for your browsers.
- Clear your browser cache before starting a Business Online session to eliminate copies of web pages stored on your hard drive. Clearing the cache depends on the browser and version you use. Find out how in your browser's preferences menu.
- Business Online will never present you with a maintenance page after you enter login credentials. Legitimate maintenance pages are displayed before entering login credentials.
- Business Online does not use pop-up windows to display login messages or errors; they are displayed directly on the login screen.
- Business Online never displays pop-up messages that say that you can't use your current browser.

Follow these General Guidelines

- Do not use public or other unsecured computers for logging in to Business Online.
- Check and verify the last login date/time every time you log in.
- Review account balances and detailed transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to Lake City Bank.
- View transfer history by viewing account activity information.
- Do not use account numbers, your Social Security Number or other account or personal information when creating account nicknames or other titles.
- Never leave your computer unattended while using Business Online.
- Never conduct banking transactions while multiple browsers are open on your computer.
- Never use shared usernames and passwords for Business Online.
- Limit administrative rights on users' workstations to help prevent inadvertently downloading malware or other viruses.
- Dedicate and limit the number of computers used to complete online banking transactions. For computers dedicated to Business Online, do not allow internet browsing or email exchange and install the latest versions and patches of both anti-virus and anti-spyware software.
- Delete online user IDs as part of the exit procedure when employees leave your company.
- Assign dual system administrators for online cash management services.
- Use multiple approvals for monetary transactions and require separate entry and approval users.
- Establish transaction dollar limits for employees who initiate and approve online payments such as ACH batches, wire transfers and account transfers.