First Citizens Community Bank

Important Notice to Online Business Banking Customers

Customers continue to look for more convenient ways to conduct their banking. In response, banks have made access to account information and the ability to complete routine transactions available through the internet and mobile devices. With this convenience comes increased risk as banks no longer have the face-to-face contact typically used to verify a person's identity. To take advantage of this trend, criminals have developed numerous methods of obtaining personal information from customers' computers, and of "taking over" online accounts to submit fraudulent transactions. The Federal Financial Institutions Examination Council (FFIEC) has issued guidelines to help banks strengthen their online security verification measures and make online transactions safer and more secure.

What you can do to help avoid online fraud

Knowledge and vigilance is the first line of defense to make sure your accounts and transactions are protected. Here are some important security tips:

- Never give your account information or online sign-on information to anyone. First Citizens will never call or e-mail you and ask you for this information.
- Don't click on attachments or weblinks contained in unsolicited e-mail messages. Phishing attempts try to trick you into revealing personal information or downloading malicious software (malware) such as keyloggers and banking trojans. Many phishing e-mails claim to be from regulatory agencies such as the Federal Reserve, NACHA, FDIC, IRS, etc.
- Install and regularly update anti-virus / anti-malware software and computer and network firewalls.
- Install security updates to operating systems and all applications as they become available.
- Select strong online banking passwords, and frequently change your passwords. Never use passwords that can be easily guessed by others.
- Regularly monitor your account activity and report any suspicious activity immediately.
- Check out these free websites for more information about internet security: www.staysafeonline.org, www.onguardonline.gov, www.ftc.gov, www.idtheft.gov.

Online business transactions generally involve accounts with large balances and the ability to move funds via ACH file origination and interbank wire transfers. This has made business accounts especially attractive targets for cyber criminals; online account takeovers and unauthorized funds transfers have increased substantially in recent years. Therefore, we recommend the following additional steps for businesses to protect their funds:

- Periodically perform a risk assessment related to your use of online banking and implement improved controls where weaknesses are found.
- Use online banking administrative accounts strictly for administration purposes; conduct all financial transactions through separate user accounts.
- Maintain employees' online banking access to reflect changes in employment status or job duties.
- Utilize online banking controls such as dual control for ACH and Wires, time restrictions, user and account restrictions, ACH processing calendars, and alerts.
- Restrict computers used for online banking from performing other online activities such as general web browsing, email, and social networking.
- Notify us anytime you submit an ACH Batch or Wire Transfer through our Cash Management system.

"Reg E" Protection

Regulation E provides consumers certain protections from unauthorized electronic transfers. Regulation E does not provide protection to business accounts.

Call Us!

If you notice suspicious activity within your account or experience security-related events such as an e-mail claiming to be from First Citizens asking for your personal information, please contact us immediately at 800-326-9486.

Revised June 2015