

FFIEC Customer Education

FFIEC Customer Education INTRODUCTION The Federal Financial Institutions Examination Council (FFIEC) recently issued new supervisory guidance designed to help make online transactions more secure. The new guidance is in response to an ever more dangerous online threat environment. Scams and hacking techniques are more sophisticated, new threats are continually being developed, and organized crime groups both in the United States and internationally have become a major force in expanding online fraud and theft. The new guidance means you may begin to see new security features on the websites you visit. Each of our online products has built-in security features which are continually enhanced in response to changing threats. Some of these enhancements are visible to you, the user, but others occur behind the scenes. The new guidance also means you will see more information on how you, as a user of online services, can take action to keep your identity and your financial information and funds secure. ***IMPORTANT INFORMATION FOR USERS OF OUR ONLINE SERVICES* FIRST COMMUNITY STATE BANK AND YOUR LOG-IN**

CREDENTIALS We will never call, email or otherwise contact you to request your access ID, password, or other log-in credentials for the online services we offer. If you receive such a request, do not provide any information. Contact a Personal Banker at 618-635-5100 to report the incident. **REPORTING SUSPICIOUS ACTIVITY** If you see suspicious activity on your account(s) or have received a suspicious call, email, letter or other similar contact regarding your relationship to First Community State Bank, call 618-635-5100 and ask to speak to a Personal Banker.

PROTECT YOURSELF BY CONTROLLING ONLINE RISKS Understand the risks of online transaction processing:- Our website includes information about preventing and reporting identity theft. The links to websites noted below provide important information and news to help you understand online transaction risk and options to help you control these risks. It is important to be informed and proactive. When it comes to internet fraud, account takeover and identity theft, an ounce of prevention is definitely worth a pound of cure. **Password Security Tips-** Do not share your User ID's or Passwords with another person or provide them to others. Safeguard your User ID and Password information—never leave the information in an unsecured location. · Create a unique User ID and Password for each site. Do not use the same identifying information on multiple websites. · Create strong User ID's and Passwords. In other words, use upper case letter(s), lower case letter(s), and numbers; if the site allows for them, use symbols as well. · Many websites force password changes (i.e. every 60 days). If a website does not do so, take the initiative and change your password on a regular basis.

Website Security Tips- Monitor account activity. View account activity online on a regular basis and review periodic account statements (monthly and/or quarterly) and reconcile them to your personal records. · Log Off from a website; do not just close the page or "X" out. · Secure websites have a web address that includes an "s" (https rather than http). If this is lacking, the site is not genuine. Do not log in or conduct business on the site. · If a website displays a security monitor, verify it has the current date. If it does not, do not use the site; it may be a spoofed or hijacked. · When completing financial transactions, verify encryption and other security methods are in place, protecting your account and personal information. **Computer / Network Security Tips-** Use quality security monitoring software on your PC that includes anti-virus, anti-malware and firewall functions. · Use your PC's security features such as individual Log-In accounts. · Keep F operating system security up-to-date by applying patches and updates. · Password-protect your computer network (physical or wireless). **Web Resources –** Learn more and do more to protect yourself online! Two user-friendly sites for users of all ages and interests:<http://onguardonline.gov/> <http://www.staysafeonline.org> Consumer alerts and tips on the FTC website:<http://www.ftc.gov/bcp/menus/consumer/data/privacy.shtml> Youth and teens and those concerned about them will find the following helpful: <http://www.lookstoogoodtobetrue.com/teen/tmain.aspx> Recent

scams and how to report scams - Go to the IC3 website, a partnership of the FBI, the National White Collar Crime Center, and the Bureau of Justice: <http://www.ic3.gov>

Scams and fraud and tips to avoid being a victim - Go to the FBI website at: <http://www.fbi.gov/scams-safety/> The identity theft page of our website has information on how to protect yourself and what to do if you suspect you are an identity theft victim. **CONSUMER PROTECTION – REGULATION E** Regulation E provides rules for error resolution and unauthorized transactions for electronic fund transfers, which includes most transactions processed online. In addition, it establishes limits to your financial liability for unauthorized electronic fund transfers. These limits, however, are directly related to the timeliness of your detection and reporting of issues to First Community State Bank. It is for this reason that we encourage you to immediately review periodic account statements and to regularly monitor your account activity online. The

"Electronic Fund Transfers" disclosure provided to you at the time of account opening provides detailed information. We will provide to you, upon request, a free printed copy of this disclosure. **ADDITIONAL INFORMATION FOR BUSINESS USERS OF ONLINE SERVICES** The new FFIEC Guidance takes note that business transactions, because of their frequency and dollar value, are inherently more risky than consumer transactions. The Guidance also notes the steep rise of online account takeovers and unauthorized online fund transfers related to business accounts in the last five years. Recently, small- to medium-sized businesses have been primary targets as cyber criminals have recognized that the security controls they have in place are not as robust as that of larger businesses. Analysis indicates enhanced controls over administrative access and functions related to business accounts and layered security using multiple and independent controls would help to reduce these types of crime. The FFIEC Guidance suggests enhanced controls for businesses:-

Business customers should be encouraged to perform a periodic risk assessment and an evaluation of the effectiveness of the controls they have in place to minimize the risks of online transaction processing. The password, website, computer and network tips above provide a starting point for this process and the web resource links provide additional detailed information. The FTC Business Center has a great deal of information for businesses at <http://business.ftc.gov/privacy-and-security/data-security>. · Business customers should understand the security features of the software and websites they utilize and take advantage of these features. Segregation of duties—the process of

separating duties so no one person can perform all steps of a transaction—is an example of a very important security feature.