



ONLINE SECURITY POLICY

While the **First Command Privacy Policy** applies whether you are online or not, we have extra measures in place to protect your privacy when you visit our Web sites and use the Internet to interact with us. These extra measures are described in this Online Security Policy.

This Online Security Policy is applicable to First Command Financial Services, Inc., and its wholly owned subsidiary companies, including First Command Financial Planning, Inc., First Command Insurance Services, Inc., First Command Advisory Services, Inc., First Command Europe Ltd. and First Command Bank.

This notice replaces any previous Online Security Policy notices provided to you by us. We may amend this Online Security Policy at any time. Please review it periodically.

If you have any questions or concerns about the privacy, security and protection of your information, you may contact First Command's Legal & Compliance Department either in writing (1 FirstComm Plaza, Fort Worth, TX 76109-4999), by e-mail (abuse@firstcommand.com), or by phone (1-800-443-2104).

A. We Work to Ensure Privacy and Security During Your Online Sessions

The information you provide to us online is protected by Secure Socket Layer (SSL technology). SSL technology is the industry- standard security protocol for data transfer on the Internet. SSL technology scrambles your information as it moves between your PC's browser and First Command's computer systems. When information is scrambled or encrypted in this way, it helps protect the safety and confidentiality of your information when you interact with us online.

B. Registered Users

When you access one of our interactive Web sites, we may request information such as your user ID and password or your email address. This information allows you to perform certain tasks (for example, correspond with us). And, it allows us to provide information you have requested. In these cases, we collect only the information necessary to interact with you.

C. Visitors

If you browse our Web sites anonymously, we do not collect, capture, or retain your personal information.

D. About Cookies

Cookies are pieces of data assigned by a Web server to the browser on your PC. Cookies help Web sites recognize return visitors. So, when you return to a Web site you've visited before, your browser gives this data back to the server. First Command uses cookies for security purposes, to facilitate site navigation, to personalize your experience while visiting our site, to determine whether you have been directed to us from another Web site, and to enhance the overall effectiveness of our site. In all cases, cookies and similar files that we place on your computer do not contain any personally identifiable information unless encrypted.

E. About Tools and Calculators

Many of the tools and calculators on our Web sites, including Command Center: Client PortalSM, are compiled using software and data from third-party providers. These tools and calculators are provided to you for information purposes only. First Command does not guarantee the accuracy, completeness or reliability of the information provided by these tools and calculators and disclaims all liability related to the use or misuse of these tools and calculators. Should you notice any incorrect information, please contact us immediately. The information provided by these tools and calculators should not be considered a recommendation or investment advice, and you should not base your financial decisions on this information.

F. About Online Banner Ads

When browsing the Internet, you may see a banner ad for a First Command product or service such as financial planning, investment services or insurance services. These ads may appear on Google or other non-First Command Web sites. We use third-party ad serving companies to serve our ad banners to sites on which we've paid to advertise. If you click on one of our ads, you are redirected to the First Command site offering that particular product or service. Sometimes these ads may contain small graphics with "tags" in them. These tags tell us how many people respond to our ads. They do not identify you personally. Instead, these tags are used only to measure the effectiveness of our ads. The companies that distribute our ads are prohibited by contract from using information other than for the agreed-upon purpose—to help us market our products and services and to measure response rates.

827-E 10/17)

© 2009-2017 First Command Financial Services, Inc., parent of First Command Financial Planning, Inc. (Member SIPC, FINRA), First Command Advisory Services, Inc., First Command Insurance Services, Inc. and First Command Bank. Securities and brokerage services are offered by First Command Financial Planning, Inc., a broker-dealer. Financial planning and investment advisory services are offered by First Command Advisory Services, Inc., an investment adviser. Insurance products and services are offered by First Command Insurance Services, Inc. in all states except Montana, where as required by law, insurance products and services are offered by First Command Financial Services, Inc. (a separate Montana domestic corporation). Banking products and services are offered by First Command Bank. Securities products are not FDIC insured, have no bank guarantee and may lose value. A financial plan, by itself, cannot assure that retirement or other financial goals will be met.

In Europe, investment and insurance products and services are offered through First Command Europe Limited. First Command Europe Limited is a wholly owned subsidiary of First Command Financial Services, Inc. and is authorized and regulated by the Financial Conduct Authority. Certain products and services offered in the United States may not be available through First Command Europe Limited.

101617

G. E-mail Safety

Use your e-mail to correspond with First Command—or anyone else—safely. E-mail is generally not a secure method of sending your personal information unless encrypted. You should never send or reply to any e-mails containing your personal information without encryption protection. If you receive an e-mail request from us containing or requesting your personal information in a non-encrypted manner, do not respond to it and notify us immediately.

To safeguard your e-mail communications with us, we have implemented an encryption system whereby you will be required to access e-mail we send to you containing sensitive information through a separate Web site. Our encryption system works as follows: You will receive an e-mail from us informing you that you have a secure message and directing you to click on a link within the e-mail. When you click on the link, your browser will open a new Web page which will ask you to enter or create a unique user ID and password. Only after you log-on with your unique user ID and password will you be able to view the secure message we sent to you.

H. Protecting Children's Privacy Online

For information about the Children's Online Privacy Protection Act (COPPA), visit the FTC Web site: www.ftc.gov. We do not knowingly collect or use personal information from children under 13 on our Web sites without parental consent.

I. Links to Non-First Command Sites

We may provide links to non-First Command Web sites. If you choose to link to Web sites not controlled by First Command, we are not responsible for the privacy or security of these Web sites, including their information collection practices or the accuracy, completeness, reliability or suitability of their information. We cannot guarantee how these non-First Command Web sites use cookies or whether they place on your computer cookies that may identify you personally. If you are asked to provide information on one of these Web sites we strongly urge you to carefully study their privacy policies before sharing your information.

J. First Command Social Media Pages

Our Social Media Public Usage Guidelines apply to your interactions with us on Facebook, Twitter, LinkedIn and other social media pages. You can review our Social Media Public Usage Guidelines for Facebook, Twitter and LinkedIn at:

<http://on.fb.me/FCguidelines> = [Facebook Usage Guidelines](#)
<https://bit.ly/fcguidelines> = [Twitter Usage Guidelines](#)
<http://bit.ly/FCFSLinkedInGuidelines> = [LinkedIn Usage Guidelines](#)

You should review these Guidelines carefully, as well as the actual social media site's privacy and security policies and settings. Importantly, you should be very cautious about placing your sensitive information on social media pages. The Internet offers no anonymity and has a long memory.

K. Transaction Requests

It is important that you do not use e-mail or voicemail to request, authorize or effect the purchase or sale of any security or product, to send fund transfer instructions, or to effect any other time sensitive transactions. Any such requests, orders, or instructions that you send will not be accepted and will not be processed. This policy is in place for your protection as it allows us to ensure that we properly verify your identity and your intentions before we take actions impacting your assets and/or policies.

L. Tips to Protect Your Information

First Command works hard to keep your information secure. You can help by following these tips to protect your information:

- ❖ Store personal information in a safe place, and tear up or shred old receipts and account statements before throwing them away.
- ❖ Change all passwords regularly. Use a mix of numbers and characters—never use common words or phrases. Your password is more secure and harder for criminals to guess if you include a special character, like an asterisk or an exclamation point.
- ❖ Protect your PINs and other passwords. Do not share them with anyone unless it's for a service or transaction you request, and you are confident the other party will protect the information as you would. Make sure your password is unique and difficult to guess.
- ❖ Maintain appropriate security on your computers and other electronic devices. Make sure you secure your wireless network and

827-E 10/17)

© 2009-2017 First Command Financial Services, Inc., parent of First Command Financial Planning, Inc. (Member SIPC, FINRA), First Command Advisory Services, Inc., First Command Insurance Services, Inc. and First Command Bank. Securities and brokerage services are offered by First Command Financial Planning, Inc., a broker-dealer. Financial planning and investment advisory services are offered by First Command Advisory Services, Inc., an investment adviser. Insurance products and services are offered by First Command Insurance Services, Inc. in all states except Montana, where as required by law, insurance products and services are offered by First Command Financial Services, Inc. (a separate Montana domestic corporation). Banking products and services are offered by First Command Bank. Securities products are not FDIC insured, have no bank guarantee and may lose value. A financial plan, by itself, cannot assure that retirement or other financial goals will be met.

101617

In Europe, investment and insurance products and services are offered through First Command Europe Limited. First Command Europe Limited is a wholly owned subsidiary of First Command Financial Services, Inc. and is authorized and regulated by the Financial Conduct Authority. Certain products and services offered in the United States may not be available through First Command Europe Limited.

protect your computers and electronic devices from viruses and spyware. Most major software companies regularly release updates or patches to their operating systems to repair security problems. You should keep your system and applications updated with the latest patches and releases. Installing a firewall is also another good idea.

- ❖ Remember to protect your personal information when disposing of computers and other electronic devices. Your computers and other electronic devices hold sensitive information like addresses and phone numbers, passwords, account numbers, email, voicemail, and text message logs. When getting rid of your old devices, it's important to take steps to help ensure this information doesn't fall into the wrong hands.
- ❖ Log out of websites. After you sign into a website, remember to sign out. This helps to ensure your information doesn't end up in the wrong hands.
- ❖ Avoiding using public wireless networks and public computers. Many cell phone carriers offer "data tethering". Consider using your cell phone's ability to access the web with your laptop or tablet instead.
- ❖ Download cautiously. If you visit a website that looks questionable, leave. Some free games and free downloads are really tricks to get you to download viruses or spyware.
- ❖ Watch out for "phishing attacks." If you receive an email that looks suspicious, don't click or open anything. Simply delete it from your inbox.
- ❖ Shop safely. If a web address begins with "https" rather than "http," it is generally secure. Avoid financial transactions on "http" sites.
- ❖ Carry only the minimum amount of identifying information you require.
- ❖ Pay attention to billing cycles and statements. Inquire if you do not receive a bill.
- ❖ Check account statements carefully to ensure all charges, checks or withdrawals are authorized.
- ❖ Guard your mail from theft. Do not leave bill payment envelopes in your mailbox with the flag up. Instead, deposit them in a post office collection box or at the local post office. Promptly remove incoming mail.
- ❖ Order copies of your credit report from each of the three major credit bureaus once a year to ensure they are accurate.
- ❖ For more on how to protect your identity, read these tips from the [Federal Trade Commission](#) and [the IRS](#).
- ❖ If you believe you are a victim of identity theft, take immediate action and keep records of your conversations and correspondence. While the steps you must take will vary with your individual circumstances, four basic actions are appropriate in almost every case:
 1. Contact the fraud departments of any one of the three major credit bureaus to place a fraud alert on your credit file:
 - Equifax (www.equifax.com): 1-888-766-0008 / P.O. Box 740241, Atlanta, GA 30374
 - Experian (www.experian.com): 1-888-397-3742 / P.O. Box 9532, Allen, TX 75013
 - Trans Union (www.transunion.com): 1-800-680-7289 / P.O. Box 2000, Chester, PA 19016
 2. Contact the creditors for any accounts that have been tampered with or opened fraudulently.
 3. File a report with your local police, or the police in the community where the identity theft took place, and get a copy of the police report.
 4. File a complaint with the Federal Trade Commission ("FTC").
 - Complaints can be filed by phone, 1-877-IDTHEFT, or through the FTC's identity theft Web site at www.consumer.gov/idtheft.