FIRST COMMAND ONLINE & MOBILE PRIVACY PRACTICES NOTICE

First Command Financial Services, Inc., and its wholly owned subsidiary companies, including but not limited to First Command Financial Planning, Inc., First Command Advisory Services, Inc., First Command Insurance Services, Inc., First Command Bank and First Command Europe Ltd. (together "First Command") are committed to protecting your privacy.

This Online & Mobile Privacy Practices Notice ("Notice") describes our online and mobile privacy practices and applies to anyone who visits our websites or branded social media sites or pages, or uses our mobile applications ("Online Services"). This notice explains which types of personally identifiable information we collect on our websites and what we do with such information, as well as the procedures for controlling what information is collected.

It should be read in conjunction with the First Command Privacy Policy and any applicable website terms and conditions of use.

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 (quality_management_inbox@firstcommand.com), or by phone (1-800-443-2104).

Each time you use our Online Services, you are indicating your acknowledgement and consent to the collection, use and disclosure of information about you collected through our Online Services as set forth in this Notice, including updates made to this Notice in the future. We may revise this Notice at any time without advance notice. We will let you know of any changes by posting a revised Notice on our website with a new effective date. If you do not accept the terms outlined in this Notice or revised Notice, please do not use our Online Services.

This Notice replaces any previous online or mobile privacy practices policy or notice provided to you by us. It is effective as of June 8, 2018.

HOW WE 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.

INFORMATION WE COLLECT & HOW WE USE IT

In general, we collect certain non-personally identifiable information when you access our Online Services.

We may also collect personally identifiable information, such as your name, mailing address, email address or telephone number, when you voluntarily provide it to us through our Online Services. We may also ask for your social security number, tax identification number, account numbers, policy numbers or driver's license number if you are completing an online form or application for our products, services and/or employment/association.

We may use and disclose your personally identifiable information that is collected through our Online Services in accordance with applicable law and the First Command Privacy Policy, including but not limited to:

- Providing and managing the online products and services you have requested;
- Verifying your identity and authenticating you;
- Protecting against fraud, security threats and otherwise managing risks;
- Communicating with you regarding products and services that may be of interest;
- Evaluating and improving our websites and other electronic offerings;
- Tailoring our services and otherwise enhancing the client experience;
- Satisfying legal or regulatory requirements or law enforcement requests; and
- As permitted or mandated by applicable law.

WAYS WE COLLECT NON-PERSONALLY IDENTIFIABLE INFORMATION:

Analytics Tracking

We employ Google Analytics and other data collection tools to collect non-personally identifiable information when available. This information is used to make improvements to our websites and to monitor the effectiveness of website changes.

Some common types of information collected include, but are not limited to, your internet protocol (IP) address; the browser type you're using; the pages you view on the website; the type of device used to access our websites and mobile apps; the items you click within the website; the state or country from which you access the website; the date and time of your visit; the name of your internet service provider; and certain demographic information Google makes available such as age, gender and interests.

This data collection provides an anonymized statistical summary that cannot be tracked back to a specific individual. For example, we are able to view the number of visitors to our site who use a certain type of Internet browser, but we are not able to determine which browser a specific visitor uses. (Please keep in mind this statement refers to general website usage, and not for instance, tools such as Command Center or OnCommand, which use personally identifiable information you have provided to us in order to better serve you and provide product support.)

By accessing our Online Services, you are allowing this information to be available to Google. Google's ability to use and share information collected by Google Analytics about your visits to our Online Services is restricted by the Google Analytics Terms of Use and the Google Privacy Policy (https://www.google.com/policies/privacy/). You can prevent Google Analytics from recognizing you on return visits to our Online Services by disabling cookies on your browser.

Cookies

A cookie is a small text file containing a string of characters sent to your computer or device when you visit a website. When you visit the website again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. Cookies can then be used to help understand how a site or service is being used, help you navigate between pages efficiently, help remember your preferences, and generally improve your browsing experience. Cookies can also help ensure marketing you see online is more relevant to you and your interests.

Cookies are uniquely assigned to you and can be read only by a web server in the domain that issued the cookie to you. Cookies are not spyware. Spyware collects and sends private information simply by being connected to the Internet without your consent. Cookies are server-specific, meaning you generally have to be on that particular site for cookies on that page to be read. Cookies can also be either temporary or persistent. A good example of a persistent cookie is when you are shopping online and you place an item in your shopping cart. When you leave the website without purchasing the item but then return to the website sometime later, if you see the item is still in your shopping cart, you have a persistent cookie on your computer from the vendor.

We, as well as our third-party vendors, including Google, may use cookies to inform, optimize and serve content based on your visit to our websites. We also may utilize cookies for advertising purposes. See the Internet Based Advertising and Analytics section below for more information.

You have the option to accept or decline cookies during Internet use. By default, most web browsers accept cookies automatically. To decline cookie use, visit the Settings menu in your browser where you may clear your browser's cookies or disable cookies. Keep in mind, this may disable certain functionality on our website and in your other Internet activities. For general visits and browsing on our website, cookies are not mandatory. However, certain tools we offer such as CommandCenter and OnCommand may require cookies for optimal use. Without cookies, we will not be able to recognize your computer or device as a returning user, meaning you may need to answer challenge questions each time you log in to CommandCenter or OnCommand.

Web Beacons or Tracking Pixels

Our web pages may contain electronic images known as web beacons or tracking pixels that allow us to count users who have visited those pages. We may include web beacons in email messages or newsletters in order to determine whether messages have been opened and acted upon. In the case of email marketing, we can track specifically which users visited certain pages on the website from an email sent to them, without otherwise collecting any other personally identifiable information.

EMAIL MARKETING

Email advertisements sent to you by us will include instructions on how to opt out of receiving such emails in the future. If you are a client and you elect to opt out of receiving email advertisements, we may still send you emails about your account relationships with us.

INTEREST-BASED ADVERTISING AND ANALYTICS

Interest-based advertising, also known as online behavioral advertising, uses information collected across multiple web sites that you visit in order to help predict your preferences and show you advertisements that are more likely to be of interest to you. When you access and use our Online Services, we or a third party vendor may send you advertisements regarding goods and services that may be of interest to you (or in some cases, to users who our service providers deem to have characteristics similar to our clients) based on information relating to your access to and use of our Online Services and other websites. To do so, we or our service providers may place or recognize a cookie on your browser (alone or in conjunction with web beacons, pixel tags or other tracking technologies).

To learn more about interest-based advertising, your choices regarding collection of your online browsing activity, or to opt out of interest-based advertising visit http://www.aboutads.info/choices and http://www.networkadvertising.org/choices . If you choose to opt out of interest-based advertising, a cookie will be placed on your browser indicating your choice. Because cookies are stored by your browser, any opt out election you make is valid only for the computer/browser combination used to opt out. Please note that even if you opt out of interest-based advertising, you may still receive advertisements from us, but they will not be customized based on your online browsing activities. Clearing your browser's cookies will remove your opt out since it is stored in a cookie, and you will need to opt out again.

Google

We use Google AdWords Remarketing and Google Analytics to advertise First Command across the Internet.

Google AdWords Remarketing will show you ads based on your past interactions with us by placing a cookie in your browser. This cookie does not in any way provide us with identifying information such as name, account numbers, social security numbers, or addresses nor does it give us access to your computer or mobile device. This cookie is used to indicate to other websites that you visited a particular page and would be responsive to ads relating to that page.

We use Google Analytics for analytics and reporting information. This information allows us to see the overall patterns of usage of our Online Services, helps us record any difficulties you have, shows us whether our advertising is effective or not, provides information about the age and gender of our website's users, along with the interests they express in their online browsing and purchasing activities, and allows us to use responses to advertisements to optimize ad performance.

You can learn about Google's practices by going to www.google.com/policies/privacy/partners/, and opt-out of them by downloading the Google Analytics opt-out browser add-on, available at https://tools.google.com/dlpage/gaoptout. If you do not wish to see ads, you can opt out of them by visiting Google's Ads Settings.

LINKS TO OTHER THIRD PARTY WEBSITES

We may place links to other non-First Command websites on our Online Services. If you choose to link to these websites which we do not control, we are not responsible for the privacy or security of these websites, including their information collection practices or the accuracy, completeness, reliability or suitability of their information. We cannot guarantee how these websites 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 websites, we strongly urge you to carefully study their privacy policies before sharing your information.

ABOUT TOOLS AND CALCULATORS

Many of the tools and calculators on our websites, including CommandCenter and OnCommand, 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.

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 CommandCenter, OnCommand or other secure website.

TRANSACTION REQUESTS

It is important that you do not use e-mail, text 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 procedure 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 insurance policies.

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.

CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA)

The Children's Online Privacy Protection Act (COPPA), as set forth by The Federal Trade Commission, prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. Accordingly, we do not intentionally collect personal information from children under age 13 on any of our websites without prior consent from their parents or legal guardians. To learn more about COPPA, please visit https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy .

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 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.
- Consider purchasing credit monitoring services or identity theft protection. These tools can help you check your credit score and reports regularly and alert you about changes and concerns. They will flag activity such as applications for credit in your name, credit limit increases or additions of authorized users on your account. Some service may also do public record searches and scans of chat rooms and black market websites for your personal data.

- 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.