CWMG Privacy and Security Policy Statement

Cornerstone Wealth Management, (CWMG) is your partner in helping you achieve your financial goals. We are dedicated to providing you with the highest level of service and protecting your privacy. As technology continues to transform the way information is collected and distributed, we want to make sure you know that we continue to implement a number of important practices for safeguarding the privacy and security of financial information about you.

- We employ safeguards to protect client information and to prevent fraud;
- We carefully manage information about you. By understanding your complete relationship with us, we can provide you with more personalized and efficient service;
- We do not sell client information to other companies for marketing purposes.

You Have Choices
You may direct us not to contact you for marketing purposes by:

- Telephone;
- Direct mail or;
- E-mail.

You may direct us not to share, within CWMG, non-transactional information about you (such as credit or employment history) that we receive from others. To exercise your choices, please contact your CWMG Wealth Advisor or visit our office at 19833 Leitersburg Pike, Hagerstown, MD 21742, or call us at 301-739-8505 to speak with a representative.

How We Secure Your Assets and Protect Information About You

We protect client data and accounts by asking you for information that only you should know when you contact us. We follow these procedures in our offices, on the phone and via the Internet.

- We train our employees to protect client information, and
- We continually enhance our security tools and processes.

How We Protect Your Privacy Online

Protecting client information is an essential part of our service to you. Our systems use technologies such as firewalls (which protect systems from intrusion) and encryption (scrambling of information) to protect client information.

How You Can Help Protect Your Privacy

Online Security Tips

- Do not share your account information or passwords with others. Do not use your Social Security number as a username or password. Change your usernames and passwords regularly and use combinations of letters, numbers, and “special characters” such as “pound” (#) or “at” (@) signs. Do not use your online brokerage password as a password for other online accounts;
- Protect your online passwords; don’t write them down or share them with anyone;
- Protect your answers to security questions. Select questions and provide answers that are easy for you to remember but hard for anyone else to guess. Do not write down your security questions or answers or share them with anyone. If you have selected security questions on other websites, avoid using the same

questions to protect your online accounts. Please note that we will never ask you to provide answers to your security questions via email;

- Use secure websites for transactions and shopping. Shop with merchants you know and trust. Make sure Internet purchases are secured with encryption to protect your account information. Look for "secure transaction" symbols like a lock symbol in the lower right-hand corner of your Web browser window or "https:// . . ." in the address bar of the website. The "s" in https indicates "secured" and means the webpage uses encryption;
- Always log off from any website after making a purchase with your credit card or debit card or other sensitive information. If you cannot log off, shut down your browser to prevent unauthorized access to your account information;
- Close your browser when you're not using the Internet;
- Be cautious when using public hotspots and consider your WiFi auto-connect settings;
- Social media is increasingly popular, but it's a good idea to keep certain personal information private. Avoid sharing personal details that are used by financial institutions to identify you, such as your birth date, home address, mother's maiden name, high school name, and pet's name. Fraudsters may use this type of information to help gain access to an account since they are common answers to security questions;
- Always carefully review the privacy options for any social network you join. The privacy options and tools for social networks can be complex and should be reviewed carefully so that there is no disclosure of information you meant to remain private;
- Do not provide confidential information online unless you initiated the contact, know the party with whom you are dealing with, and provide the information through a secure channel;

Computer Security Tips

- Avoid downloading programs from unknown sources;
- Keep your computer operating system up-to-date to ensure the highest level of protection;
- Install a personal firewall on your computer;
- Install, run, and keep anti-virus and other software updated;
- Turn your computer off completely when you are finished using it – do not leave it in sleep mode;
- Be wary of conducting online banking activities on computers that are shared by others. Public computers (computers at internet cafes, copy centers, etc.) should be used with caution, due to shared use and possible tampering. Online banking activities and viewing or downloading documents (statements, etc.) should be conducted when possible, on a computer you know to be safe and secure;
- Ensure your computer operating system, software, browser version and plug-ins are current. Before downloading an update to your computer program, first go to the company's website to confirm the update is legitimate;
- Configure your devices to prevent unauthorized users from remotely accessing your devices or home network. For example, if you use a home wireless router for your home internet connection, follow the manufacturer's recommendations to configure the router with appropriate security settings.

Email Security Tips

- Be wary of suspicious e-mails. Never open attachments, click on links, or respond to e-mails from suspicious or unknown senders;
- If you receive a suspicious e-mail that you think is a phish e-mail, do not respond or provide any information.

General Fraud Prevention Tips - Follow these tips to help protect yourself from fraud:

- Carry only necessary information with you. Leave your Social Security card and unused credit cards at home in a safe and secure location;

- Make photocopies (front and back) of vital information you carry regularly and store them in a secure place, such as a safety deposit box. Then, if your purse or wallet is lost or stolen, you have contact information and account numbers readily available;
- Do not provide your Social Security number unless absolutely necessary;
- If you are uncomfortable with a phone call that was not initiated by you, hang up or ask for the purpose of the call. Then contact the company using legitimate sources such as contact phone numbers found on the company's website, your bank statements, and those listed on your ATM, debit, or credit card;
- Never provide payment information on a call that you didn't initiate;
- Replace paper invoices, statements, and checks with electronic versions, if offered by your employer, bank, utility provider, or merchant;
- If you have an online account, you can reduce paper statements by signing up for online statements;
- Shred documents containing personal or financial information before discarding. Many fraud and identity theft incidents happen as a result of mail and garbage theft;
- Review your credit report at least once a year, looking for suspicious or unknown transactions. Please refer to the section "Identity Theft Assistance" below;
- Promptly retrieve mail and place outgoing mail in a U.S. Postal Service mailbox instead of your home mailbox, to reduce the chance of mail theft. Consider paperless options for your bills and financial statements;
- Know your billing and statement cycles. Contact the company's customer service department if you stop receiving your regular bill or statement.

If you believe you are a victim of fraud or identity theft, please contact us at 888-321-0808 for assistance, such as to put holds on your accounts. Also, see the Identity Theft Assistance section of our Privacy Statement below.

How We Gather Information to Understand Your Financial Needs

The information we gather about you helps us to better understand your financial needs and to provide more personalized, efficient service to you. For example, the information you give us will allow us to process your requests and transactions, to recommend investment products, or to evaluate your financial needs.

The information we gather comes from a variety of sources, including:

- Information you provide to us (such as information on applications about assets and income);
- Information related to your transactions with us and our affiliates (such as account balance and payment history);
- Information we receive from credit reporting agencies and other companies when you apply for a service (such as your credit history);
- Information we obtain from others at your request (such as information about assets held at another institution for inclusion in a financial plan).

Information obtained when you use Internet products and services (such as application and transaction information and information contained in emails you send us). We carefully manage all the information gathered about you as described in the following section.

How We Manage Information to Serve Your Needs

We consolidate information about clients, including:

- Information based on your transactions with us (for example, information that we would consolidate from your accounts if you wished to make an automatic mortgage payment from your checking account) and contact information (such as your name and address);
- Non-transactional information received from others (such as credit or employment history) to evaluate your eligibility for various financial services.

You may tell us not to share non-transactional information with other companies. For more information, see the section below entitled, "Your Choices as a Client."

Outside of Cornerstone Wealth Management
With limited exceptions like those below, we do not provide client information to companies outside of CWMG. You do not need to request this confidentiality; it is our standard practice.

In order to serve your needs, we may provide all of the information we gather to:

- Specialists that perform business operations for us (such as printing services);
- Companies that act on our behalf to market our services, or companies with whom we have entered into a joint marketing agreement in order to provide you with valuable financial services that we do not offer (such as annuities);
- Others only as permitted or required by law (such as to protect against fraud or in response to a subpoena).

We select very carefully the companies that provide services on our behalf, or offer you financial services that we do not provide. Also, we only provide them with information that we believe is necessary to fulfill their responsibilities or to provide a financial service to you. These companies are prevented by legal agreement from using this information for their own purposes or selling this information to others.

CWMG will not share your personal information with others except as stated in this Policy, unless we give you additional notice or ask for your permission. CWMG reserves the right to disclose or report the personal information in certain circumstances: (1) to CWMG's clearing firm, or other qualified custodians used by CWMG as we deem necessary or appropriate, to handle, process and clear transactions in accounts; (2) where we believe in good faith that disclosure is required by law, to cooperate with regulators or law enforcement authorities; (3) to perform necessary credit checks or collect or report debts owed to us; (4) to protect our rights or property; (5) upon reasonable request by a mutual fund company or relating to other investments in your account(s).

CWMG does not sell its customers' or potential customers' personal information.

Your Choices as a Client

We are committed to helping you manage your finances effectively and enhance the returns on your financial investments. For these reasons, we may contact you to offer financial advice and inform you of different options that may be of value to you. If you are comfortable with the ways in which we contact you currently, there is no need to indicate your preferences. We recognize, however, that you may wish to limit the ways in which we contact you for marketing purposes and we offer the options listed below:

- Please do not contact me by telephone for marketing purposes;
- Please do not contact me by mail for marketing purposes;
- Please do not contact me by e-mail for marketing purposes.

You also have a choice about how information about you is managed within CWMG. If you prefer that we do not share non-transactional information about you with other companies, you may choose the following option:

- Please do not share, among other companies, non-transactional information about me that you receive from others.

Whatever your preferences, we will honor your wishes and respect your privacy. Your preferences will remain in effect until you tell us otherwise. You do not need to notify us if you have already indicated your preferences to us.

To discuss your options, inform us of a preference, or provide us with feedback, contact your CWMG Wealth Advisor, visit our office, or call us at 301-739-8505. If you contact us, we will assume your preferences apply to you only – unless you tell us that they also apply to other individuals listed on your account(s).

Please note that we are committed to providing you with superior service. Occasionally, we may need to contact you to resolve a problem or to service your accounts. For example, if we observe unusual activity in your account, we may contact you to verify your transactions and confirm that they are authorized.

Identity Theft Assistance

Monitoring your credit for accuracy and to make sure it is being reported correctly are important steps you can take to protect yourself from fraud and identity theft. By law, you are entitled to receive one free credit report every 12 months from each of the nationwide consumer credit reporting companies (see below). To learn more or request a copy of your credit report, you can visit https://www.annualcreditreport.com, or call 877-322-8228.

Report Fraud and Identity Theft

Fraud is usually limited to an isolated attempt to steal money from an existing account, such as a charge on a stolen credit card. Identity theft occurs when someone steals your personal information and uses it to open new accounts or initiate transactions in your name.

If you believe you may be a victim of identity theft:

- Contact Cornerstone Wealth Management Group immediately at 301-739-8505 to place holds on your accounts;

- Contact the major credit bureaus. You can request that the three main credit bureaus place a short or long-term fraud alert on your credit file. This alert requires creditors to verify your identity before opening any new accounts in your name or changing any existing accounts. You will only need to contact one bureau, which will notify the others.

  Credit bureaus must provide victims of identity theft a free copy of their credit report. You should request one from each bureau, as the information can differ. Review your credit reports carefully for fraudulent activity. If fraud has occurred, notify the credit bureau and the companies where accounts were opened to report the fraud directly.

  Once a dispute has been resolved, the credit bureaus you contacted will send you another copy of your credit report. Review the report to make sure that all fraudulent activity has stopped and your file has been corrected.

  For more information about the steps to take and for credit reports, contact

  - Experian: 888-397-3742 or www.experian.com
  - Equifax: 888-766-0008 or www.equifax.com
  - Trans Union: 800-680-7289 or www.transunion.com

- Contact other creditors. Contact your other creditors, including credit card and phone companies, banks, and other lenders, to notify them of potential fraud or identity theft. Consider following up your telephone conversations with a letter. Close any accounts that have been breached and reopen them with new account numbers and passwords. Do not use your Social Security number as a username or password.

- File a report with the police in your local jurisdiction if you suspect that your personal or financial information was stolen. Retain the report number and the name of the officer who took the report. A

police report may lend credibility to your case when dealing with creditors, who may require proof of criminal activity.

- Report the criminal activity to the Federal Trade Commission (FTC) by contacting the FTC's Identity Theft Hotline at 877-IDTHEFT (877-438-4338) to speak with a trained identity theft counselor or you can submit a complaint to the FTC on their website, www.ftc.gov/.

- Contact other agencies as appropriate.
    - Postal Inspection Service: www.usps.com. If you believe your mail was stolen or redirected, notify your local post office.
    - Social Security Fraud Hotline: 1-800-269-0271. If you suspect someone is using your Social Security number for fraudulent purposes, call the hotline.
    - Department of Motor Vehicles: If you believe someone is trying to get a driver's license or identification card using your name and information, contact your local DMV.

- Carefully review all your accounts. Since identity theft takes time to resolve, you should continue to review all charges and transactions appearing on account statements and online. Immediately report any discrepancies.

How to Limit Direct Marketing from Other Companies

To limit the instances in which credit reporting agencies share your information with companies wishing to offer you pre-approved credit solicitations, you can call 888-567-8688 (the Credit Reporting Industry Pre-screening Opt Out Number), or visit https://www.optoutprescreen.com/?rf=t.

To limit the marketing materials you receive from companies outside CWMG, you may contact the Direct Marketing Association at the address below and have your name removed from their contact lists. You must include your name, address, telephone number, and signature with your request.

Direct Marketing Association, Inc.
1111 19th Street, Suite 1100
Washington, DC 20036-3603

The Direct Marketing Association utilizes a website to help you get off commercial email lists. Their email address is http://www.dmaconsumers.org.

You may also limit telemarketing calls from companies outside CWMG by adding your telephone number to the National Do Not Call Registry. Their website is http://www.donotcall.gov, where you can register your telephone number(s) as well as file a complaint.

We Strive to Maintain Accurate Information

We strive to maintain complete and accurate information about you and your accounts. If, at any time, you believe that our records contain inaccurate or incomplete information about you, please let us know immediately. We are committed to resolving any inaccuracies as quickly as possible.

Credit Reporting Agencies

If you believe we have reported inaccurate information about your account to any credit reporting agency, please let us know in writing. Be sure to include your complete name, current address, Social Security Number, telephone number, account number, type of account, specific item of dispute, and the reason you believe the information is wrong. Send your notice to Cornerstone Wealth Management Group, Attn: Compliance, 19833 Leitersburg Pike, Suite 100, Hagerstown, MD 21742. We will investigate your concern and correct any inaccuracies we find. We will inform you of any actions we take.

Security Standards

Protecting your personal information online is vital. We go to great lengths to see that your transactions and personally identifiable information are confidential, secure, and protected from loss, misuse, alteration or destruction.

Other Important Information

Financial advisors ("FA") may change brokerage and/or investment advisory firms and non-public personal information collected by your FA may be provided to the new firm so your FA can continue to service your account(s) at the new firm. If you do not want your financial advisor to use or transfer this information, please call 888-321-0808 to opt out of this sharing. Opt-in states, such as California, Massachusetts, Maine, Alaska, New Mexico, North Dakota, or Vermont, require your affirmative consent to share your non-public information with the FA's new firm, and in those states, you must give your written consent before the FA can take your non-public information with him or her. You can withdraw this consent at any time by contacting 301-739-8505.

Information for Vermont and California Customers

In response to a Vermont regulation, if we disclose personal information about you to non-affiliated third parties with whom we have joint marketing agreements, we will only disclose your name, address, other contact information, and information about our transactions or experiences with you.

In response to a California law, we automatically treat accounts with California billing addresses as if you do not want to disclose personal information about you to non-affiliated third parties except as permitted by the applicable California law. We will also limit the sharing of personal information about you with our affiliates to comply with all California privacy laws that apply to us.

About This Statement

This Privacy and Security Statement explains how CWMG handles and protects customer information. This Statement applies to consumers who are customers or former customers of CWMG.

We may change this Statement from time-to-time based on our need to accurately reflect how we gather and manage customer information. All changes to this Statement will be effective upon posting on http://www.carsonwealth.com.

If You Have Questions, Contact Us

We welcome the opportunity to answer any questions you may have about this Statement or the safeguarding and confidentiality of your information. For more information, contact your CWMG Wealth Advisor, visit our office, or call us at 301-739-8505 to speak to a representative.