

2019 Notice to Clients Brown Advisory Securities

At Brown Advisory Securities, LLC (“Brown Advisory” or the “Firm”), we believe that you deserve frank and open communication on all aspects of our relationship. In this spirit, we provide this annual summary of our policies relating to confidentiality and privacy of client information, conflicts of interest, margin disclosure, Form ADV, other regulatory notices, and information for our managed account clients.

Confidentiality and Privacy Policy (Regulation S-P and S-AM Notice)

Brown Advisory takes the confidentiality of your personal information and the privacy of your account very seriously. Our commitment to safeguard your personal information goes beyond our legal obligation to process your transactions accurately and securely. Whether we serve you online, in person, on the telephone or by mail, the principles that guide the way in which we conduct business are built upon our core values of trust and integrity.

To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include physical, electronic and procedural safeguards that are designed to protect your personal information, including various measures to protect such information while it is stored electronically. We train and consistently remind all employees to respect client privacy (including the identity of our clients) and to recognize the importance of the confidentiality of such information. Those who violate our privacy policy are subject to disciplinary action.

Federal law (Regulations S-P and S-AM) requires us to inform you that we have on record personal information about you and that we obtain such information from you directly (e.g., information you provide to us on account applications and other forms, such as your name, address, Social Security number, occupation, risk tolerance, assets and income) and indirectly (e.g., information on our computer systems about your transactions with us, such as your account balance and account holdings). All personal information is kept confidential.

Like all investment firms, in order to better serve clients, Brown Advisory needs to share certain nonpublic personal information in the normal conduct of our business with other members of the Brown Advisory corporate group and with unaffiliated companies with whom we have service agreements. We may share your personal information in order to process transactions, maintain your accounts(s), and offer our products and services to you. This sharing allows us to: (i) provide better and more complete investment and strategic advice; (ii) develop new services that meet additional needs you may have; and, (iii) comply with legal and regulatory requirements. When we share information with companies not affiliated with us that are under contract to perform services on our behalf, such as vendors that provide services directly related to your account relationship with us, our agreements with these companies require that they keep your information confidential and not use such information for any unrelated purpose. We may also be required to share nonpublic personal information to respond to court orders and legal investigations and in connection with regulatory requirements.

We do not sell information about you to third parties, we do not jointly market with non-affiliated financial companies, and we do not otherwise disclose information about you to non-affiliates so they can market to you.

If you are a new client, we can begin sharing your information internally for marketing purposes 30 days from the date you are provided with this notice. When you are no longer our client, we continue to share your information as described in this notice. You may limit our ability to share information internally with other members of the Brown Advisory corporate group for marketing purposes by calling 410-537-5380 or by emailing optout@brownadvisory.com. If you opt out, your selection will be treated as permanent unless you tell us otherwise.

Pursuant to Section 503 of the Gramm-Leach-Bliley Act, this notice may be reduced or eliminated in future years. However, our Confidentiality and Privacy Policy will remain in effect and is available for your review at any time at <https://www.brownadvisory.com/us/disclosures> or by contacting your Client Service team. We will provide notice to you in case the Policy changes or as otherwise required by law.

Identify Theft Program (Regulation S-ID)

Federal regulators have adopted rules and guidelines that require certain regulated entities to establish programs to address risks of identity theft. These "Red Flags Rules" require certain SEC-regulated entities to develop and implement a written program designed to detect, prevent, and mitigate identity theft in connection with certain customer accounts.

Brown Advisory's policy is to protect you and your accounts from identity theft and to comply with the SEC's Red Flags Rules. Our identity theft program is designed to identify relevant identity theft red flags, detect those red flags, respond appropriately to any red flags that are detected, and prevent and mitigate identity theft. Brown Advisory's identity theft policies, procedures and internal controls are reviewed periodically and updated as necessary to ensure that they account for changes both in regulations and in our business. This program overlaps with and leverages other relevant firm policies and programs, such as our Anti-Money Laundering Program ("AML") and policies and procedures pursuant to Regulation S-P, among others.

To identify relevant identity theft red flags, Brown Advisory considers general factors, such as types of client accounts and the methods by which such accounts can be opened or accessed. Detection of red flags is based on the methods of obtaining information regarding clients or transactions and verifying such information pursuant to AML or other procedures. Brown Advisory has in place policies, procedures and practices with respect to confidentiality, safeguarding of client information and system controls which, among other purposes, are designed to prevent and mitigate identity theft. However, even the most well designed controls cannot guarantee complete protection. The best protection against identity theft is vigilance and care by both Brown Advisory and clients.

Upon detecting an incident of actual or attempted identity theft, we will notify you and may report the incident to relevant regulatory or law enforcement agencies, as appropriate. Brown Advisory's senior management and Board of Directors receive reports on a periodic basis regarding issues pertaining to this program.

Conflicts of Interest

We may recommend that you purchase (or hold) a Brown Advisory mutual fund, private fund or other product in connection with your relationship with the Firm, or we may refer you to one of our investment advisory affiliates for investment management or other services. In each of these circumstances, your Financial Advisor may receive compensation for the sale (or holding) or referral to our affiliates.

Margin Disclosure Statement

When you buy securities on margin, those securities are collateral for the loan to you. If the securities in your account decline in value, so does the value of the collateral supporting your loan, and, as a result, the Firm can take action, such as issue a margin call and/or sell securities or other assets in any of your accounts with us, in order to maintain the required equity in the account. It is important that you fully understand the risks involved in trading securities on, or otherwise using, margin.

These risks include, but are not limited to, the following:

- You can lose more funds than you deposit in the margin account.
- The Firm can force the sale of securities or other assets in your account(s).
- The Firm can sell your securities or other assets without contacting you.
- You are not entitled to choose which securities or other assets in your account(s) are liquidated or sold to meet a margin call.
- The Firm can increase its "house" maintenance margin requirements at any time and is not required to provide you advance written notice.
- You are not entitled to an extension of time on a margin call.

Other Regulatory Notices

You may view additional disclosures related to our Business Continuity Plan, the routing of customer orders, and information we collect to aid in combating money laundering and terrorist activity (New Account Notification) on our website located at www.brownadvisory.com.

We hope that this explanation of certain of our policies is helpful to you. If you have any questions concerning any of these disclosures, please call your Client Service team.

For Our Clients with Managed Accounts

Form ADV

The Firm is a registered investment adviser. Annually, clients will receive updates to Form ADV Part 2A in one of two ways: 1) a complete copy of Form ADV Part 2A accompanied by a summary of material changes, or when appropriate, 2) a summary of material changes along with an offer to provide a complete copy of Form ADV Part 2A upon request. Clients may request a copy of Form ADV Part 2A at any time without charge by sending a written request to our Chief Compliance Officer at our Baltimore address, or by email to compliancegroup@brownadvisory.com.

Annual Contact

If there have been any changes in your financial situation or investment objectives, or if you wish to impose or modify any reasonable restrictions on the management of your account, we request that you promptly notify your Financial Advisor.

Proxy Voting

Unless otherwise delegated by a client and agreed to by Brown Advisory Securities, the client and not the Firm will be responsible for voting proxies of securities held in the client's account. At all times, clients have the right to vote securities or delegate the authority to vote securities to another person. Accordingly, Brown Advisory, as a matter of policy and practice, does not have any responsibility for voting proxies for clients' portfolio securities.

Cash Management Options

From time to time, Brown Advisory uses money market funds, and cash sweep products offered by banks and broker-dealers, as cash management options for discretionary client accounts. These cash management options are (i) selected, in the case of money market funds, and (ii) monitored, in the case of money market funds and sweep vehicles, by Brown Advisory's manager research team, which is responsible for evaluating the investment merits of third party investment options available to our clients. Sponsors of certain of these cash management options have agreed to pay Brown Advisory a fee, typically a percentage of invested assets, for providing reporting and other administrative services to our clients that invest therein. This fee, which does not affect the investment return of the respective investment option, creates a potential conflict of interest because it provides an incentive for Brown Advisory to use such cash investment option for our clients. Brown mitigates this conflict by ensuring that the manager research team evaluates investment options solely based on the objective investment merits of a particular investment option; these administrative services payments do not factor into the manager research team's evaluations about the cash investment options that are made available to Brown Advisory's clients. The range of cash management options may vary based on the custodian selected by the client.

Wells Fargo Clearing Services

One of the cash management options noted above is a Bank Deposit Account at Wells Fargo Clearing Services, LLC, which is utilized by Brown Advisory Securities as a cash sweep vehicle for certain eligible accounts. Wells Fargo Clearing Services, LLC has agreed to pay Brown Advisory a fee for providing reporting and other administrative services to clients that invest therein. This fee does not affect the investment return of the Bank Deposit Account.

Fraud and Identify Theft Assistance

If you believe you are a victim of fraud or identity theft, please contact your Client Service Team for assistance. This may include placing holds on your accounts or changing account number information. Additional measures you can take include the following:

- Contact all financial services firms with whom you maintain accounts for assistance, such as placing holds on your accounts.
- Contact the Social Security Administration's Fraud Hotline at 1-800-269-0271 to report fraudulent use of your identification information.
- Report the incident as quickly as possible to each of the credit reporting agencies below:
 - Experian 1-888-397-3742**
 - Equifax 1-800-525-6285**
 - TransUnion 1-800-680-7289**
- File a police report in your local jurisdiction and retain the report number and the name of the officer who took the report.
- File a complaint with the Federal Trade Commission (FTC) by contacting the FTC's Identify Theft Hotline: 1-877-IDTHEFT

Information Technology Security

We employ strong protective measures to safeguard your personal and other information from unauthorized access or use. We are committed to maintaining security designed to protect our systems from malicious activity.

If you have reason to believe that your interaction with us has been compromised, please contact your Brown Advisory Securities Client Service Team for assistance.

In addition to Brown Advisory taking steps to protect clients in their interactions with us, your Brown Advisory Securities Client Service Team can offer helpful tips and tools to help you protect your personal data and enhance your information security generally.

How to Protect Yourself

We recommend that you follow these security measures to protect and help prevent potential misuse of personal information about you:

- Protect and properly dispose of your account records.
- Do not share account information, passwords, user IDs, PINs, code words, or other confidential information with others.
- Do not provide confidential information by telephone to unknown callers.
- Do not provide confidential information online unless you initiate the contact, know the party with whom you are dealing, and provide the information through a secure channel.
- Do not send sensitive information via unencrypted e-mail.
- When conducting business over the internet, always use a secure browser, exit online applications as soon as you finish using them, and make sure you keep your computer and software up to date with the latest security software.
- Monitor your financial accounts often for suspicious activity.
- Monitor your credit report for accuracy. By law, you are entitled to receive one free credit file disclosure every 12 months from each of the nationwide consumer credit reporting companies. To learn more or request a copy of your credit report, visit <http://www.annualcreditreport.com> or call 1-877-322-8228.

Contact Your Brown Advisory Securities Team With Questions

We welcome the opportunity to answer any questions you may have about this statement or the safeguarding and confidentiality of client information. Please contact your Brown Advisory Securities Client Service Team for additional information or to discuss any concerns.