

Other Website Disclosures

USA Patriot Act Customer Identification Program Notice

Important Information You Need to Know About Opening a New Account

To help the government fight the funding of terrorism and money laundering activities, federal law requires financial institutions to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

Financial Exploitation of Seniors and Specified Adults

FINRA member firms, which include Brown, may place a temporary hold on requested disbursements of funds or securities, from the account of specified customers, where there is a reasonable belief of financial exploitation.

Effective February 2018, a new designation, called a trusted contact person (TCP), was instituted in the financial services industry. The TCP is intended to be an alternate contact/resource for the member firm, if necessary, in administering the account of a senior customer (age 65 & over) or a specified adult (age 18 or older perceived to have a mental or physical impairment, who is unable to protect his or her interests). The firm may contact the TCP when the latter cannot be contacted after multiple attempts, or if it is believed there could be diminished mental or physical capacity, or if it is believed a financial exploitation may be occurring. The TCP may retrieve or relay personal important information, on behalf of the customer. Interested account owners may obtain a copy of the "Trusted Contact Person form" by contacting us.

Additionally, FINRA has developed a Securities Helpline for Seniors. If you are a senior investor, you may call 1-844-57-HELPS (844-574-3577) Mon-Fri 9 a.m.-5p.m Eastern time, if you feel you need assistance from FINRA, or to raise concerns about issues with your brokerage account investments.

Identity Theft Policy

What to do if you're a victim of Identity Theft

If you are a client of and feel you may be a victim of identity theft, please contact your financial professional immediately.

In addition, take the following **four steps** as soon as possible, and keep a record with the details of your conversations and copies of all correspondence.

1. Place a fraud alert on your credit reports, and review your credit reports.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.

- **TransUnion:** 1-800-680-7289
www.transunion.com
Fraud Victim Assistance Division,
P.O. Box 6790, Fullerton, CA 92834-6790
- **Equifax:** 1-800-525-6285
www.equifax.com
P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian:** 1-888-EXPERIAN (397-3742)
www.experian.com
P.O. Box 9532, Allen, TX 75013

2. Once you place the fraud alert, you're entitled to order one free copy of your credit report from each of the three consumer reporting companies, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like your Social Security number, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. See [Disputing Errors On Your Credit Report](#).

Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

3. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, use the sample letter to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquires" NOT the address for sending your payments.
- You can also use the FTC's resources to create a recovery plan. The IdentityTheft.gov website will walk you through each step of the recovery process, track your progress, and even pre-fill forms and letters for you.
- Filing a report with the police and then providing the company with an Identity Theft Report will give you greater protection. For example, if the company has already reported these unauthorized accounts or debts on your credit report, an Identity Theft Report will require them to stop reporting that information. Use the cover letter to explain to the company the rights Identity Theft Report.

4. Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

5. File a complaint with the Federal Trade Commission.

You can file a complaint with the FTC using the online complaint form; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Be sure to call the hotline to update your complaint if you have any additional information or problems.

By sharing your identity theft complain with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violation of laws the agency enforces.

Additionally, you can provide a printed copy of your online Complaint form to the police to incorporate into their report. The printed FTC ID Theft Complaint, in conjunction with the police report, can constitute an identity Theft Report and entitle you to certain protections. This Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit report; (3) prevent a company from continuing to collect debts that result from identity theft; and (4) place an extended fraud alert on your credit report.

6. File a report with your local police or the police in the community where the identity theft took place.

Call your local police department and tell them that you want to file a report about your identity theft. Ask them if you can file the report in person. If you cannot, ask if you can file a report over the Internet or telephone. See below for information about Automated Reports.

If the police are reluctant to take your report, ask to file a "Miscellaneous Incident" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

When you go to your local police department to file your report, take a printed copy of your FTC ID Theft Complaint form, your cover letter, and your supporting documentation. The cover letter explains why a police report and an ID Theft Complaint are so important to victims.

Ask the officer to attach or incorporate the ID Theft Complaint into their police report. Tell them that you need a copy of the Identity Theft Report (the police report with your ID theft complaint attached or incorporated) to dispute the fraudulent accounts and debts created by the identity thief. (In some jurisdictions the officer will not be able to give you a copy of the official police report, but should be able to sign your Complaint and write the police report number in the "Law Enforcement Report" section.)

SIPC Notice

Brown & Brown Securities, Inc. (BBSI) is registered with the Securities and Exchange Commission (SEC) and Texas State Securities Board as a broker-dealer and is a member of the Financial Industry Regulatory Authority, Inc. (FINRA), the Securities Investor Protection Corporation (SIPC) and the Municipal Securities Rulemaking Board (MSRB). BBSI is affiliated with Brown & Brown Financial Services, Inc. (BBFSI) an investment adviser registered with the SEC, by way of common control.

In the event of a Brown's failure, SIPC protects its members' securities customers up to \$500,000 (including \$100,000 for claims for cash). You may obtain an explanatory brochure by contacting SIPC at (202) 371-8300, visiting SIPC's website at www.sipc.org or by asking your Registered Representative. Each customer account carried by Brown also receives excess SIPC protection. Neither SIPC coverage nor excess SIPC coverage applies to market losses.

Customer Complaint Notification

If you have a customer complaint, your request may be made in writing addressed and mailed to: Brown & Brown Securities Inc., 6440 North Central Expressway, Suite 107 Dallas, TX 75206 or you may call our main office by calling (214) 696-1768.

SEC Order Routing Disclosure/ Quality of Execution Notice

Midland Securities, Ltd. is a fully-disclosed correspondent of Hilltop Securities, Inc.

Please refer to this hyperlink for order-routing information.

The Securities & Exchange Commission (SEC) adopted Rule 606 (formerly SEC 11Ac1-6) of the Securities Exchange Act. Rule 606 requires Brown & Brown to comply with four primary disclosure elements: 1.) to make publicly available quarterly reports that present a general overview of order routing practices; 2.) to disclose the nature of any relationship it has with venues that it routes client orders; 3.) to furnish clients upon request the venues to which individual orders were sent for execution for the previous six months; and 4.) to provide an annual written notification to clients that this information is available upon request.

With respect to Brown's relationships with trading venues, Brown directs all trades in over-the-counter (OTC), listed stock, and options to our clearing firm, Hilltop Securities, for execution.

Hilltop, receives compensation for directing OTC and equity stock, and listed options order flow, to selected market makers and option specialists. Hilltop also directs a percentage of listed equity flow to certain exchanges or specialists and receives compensation in connection with the routing of such orders.

If you have any questions regarding this information, you may contact Brown & Brown Securities Inc., 6440 North Central Expressway, Suite 107 Dallas, TX 75206 or you may call our main office by calling (214) 696-1768.

Municipal Securities Rulemaking Board ("MSRB") Annual Notice

Brown & Brown is registered with the U.S. Securities and Exchange Commission and the Municipal Securities Rulemaking Board.

Website address for the Municipal Securities Rulemaking Board is www.msrb.org.

An investor brochure is available at <http://msrb.org/msrb1/pdfs/MSRB-Investor-Brochure.pdf>. Among other information, the brochure describes the protections that may be provided by the Municipal Securities Rulemaking Board rules and how to file a complaint with an appropriate regulatory authority.

5/5/22