June 27, 2014

[name
Address
City, state, zip]

Dear Client:

Sterne, Agee & Leach is contacting you because we have learned of a data security incident that occurred between May 29th and 30th, 2014, which may have resulted in an unauthorized person acquiring access to personal information we maintain relating to your brokerage account.

An employee of Sterne, Agee & Leach ("Firm") was unable to locate their firm-issued laptop. While the laptop was password protected, the data stored locally was not encrypted. The data stored locally included data compiled for mailing to certain Private Client Group customers whose accounts were open as of May 29, 2014 and may have included account information maintained by Sterne Agee & Leach for past and present customers whose accounts were opened between July 1, 1992 and June 30, 2013. The subject data may have included personal information such as name, address, account number and social security numbers. This data DID NOT include date of birth, account holdings, account passwords or access codes.

The Firm conducted an immediate investigation, with a focus on both finding the laptop and determining if it had been used to access additional data not stored locally. We were able to conclude that the laptop has not been used to access the Firm's servers but cannot conclude whether the laptop has been turned on and the data stored locally accessed. There is the risk, therefore, of an unauthorized acquisition of your personal information. The Firm has filed a police report relating to this incident. While we are confident that this was an isolated incident, we have taken additional steps to secure all customer data: all laptops are now encrypted, data information security policies have been enhanced and employees have received additional instruction on data security protocols and compliance.

The confidentiality of customer data is of utmost importance to us, and we apologize for any inconvenience or concern this issue may cause you. To minimize or eliminate potential harm and help protect your identity, we are offering all potentially impacted customers a one-year membership to Experian's® ProtectMyID® Alert at no cost to you. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: September 30, 2014 (Your code will not work after this date.)
2. VISIT the ProtectMyID Web Site to enroll: www.protectmyid.com/redeem
3. PROVIDE Your Activation Code: [code]

Additional Details Regarding ProtectmyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- Free copy of your Experian credit report
- Surveillance Alerts for:
  - Daily Bureau Credit Monitoring: Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- Identity Theft Resolution & ProtectMyID ExtendCARE: Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARETM, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.

- $1 Million Identity Theft Insurance* : Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items.

If you have questions regarding this incident, the information in this letter or need assistance in enrolling in the ProtectMyID® service, please call 800-357-0823 and provide engagement #: PC85704.

You can also take the following additional precautionary steps to further protect yourself:

Remain vigilant - We encourage you to remain vigilant by reviewing your account statements and free credit reports.

If you discover errors or suspicious activity on your credit card account, you should immediately contact the credit card company and inform them that you have received this letter. Confirm the address they have on file for you is your current address, and that all charges on the account are legitimate.

To obtain an annual free copy of your credit reports, visit www.annualcreditreport.com or call 1-877-322-8228. Review your credit reports carefully for inquiries from companies you did not contact, accounts you did not open or debts on your accounts that you do not recognize. Also make sure to verify the accuracy of your Social Security Number, address(es), complete name and employer(s) information. If information on a report is incorrect, notify the credit bureau directly using the telephone number on the report.

Additional contact information for the major credit bureaus is as follows:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2002	P.O. Box 105281
Atlanta, GA 30374-0241	Allen, TX 75013	Springfield, PA 18064-0390
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Consider placing a fraud alert on your credit file. A fraud alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for credit, it might protect against someone else obtaining credit in your name.

Consider placing a security freeze on your credit file. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

Identity Theft Assistance - Report suspected incidents of unauthorized activity promptly to your financial institution, local law enforcement, your Attorney General, or the Federal Trade Commission.

The FTC can be reached at: 600 Pennsylvania Avenue NW, Washington DC 20580, www.ftc.gov, or by calling 1-877-ID-THEFT (1-877-438-4338).

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001, 91-716-6400, www.ncdoj.gov.

Sincerely,

Eric D. Needleman, CEO

* Identity theft insurance is underwritten by insurance company subsidiaries of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.