USAA®
9800 Fredericksburg Road
San Antonio, Texas 78288

August 1, 2014

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol St.
Concord, NH 03301

Dear Attorney General Foster:

We are writing to notify you of a data security incident impacting New Hampshire residents. At this time, we believe four New Hampshire residents were impacted, but we are continuing to investigate whether any additional New Hampshire residents were impacted. On July 26, 2014, a technical, programming error occurred when some USAA members accessed usaa.com or USAA's mobile application allowing these USAA members to potentially view another USAA member's personal information. This error occurred when any two members logged on at the exact same time and into the same server. Depending on the type of products owned and services used by these members, the following personal information may have been viewed: first and last name, address, SSN (if certain documents were posted to a member's online documents account), checking and savings account numbers and transactions, loan balances and general information, insurance policies, and other general information available through usaa.com and USAA's mobile application.

USAA learned of the error within 10 hours of the occurrence and immediately corrected the system error. The affected New Hampshire residents will be mailed a notification letter informing them of the incident, and a copy of the notice is attached for your reference. We expect to mail the letter to New Hampshire residents no later than 8/8/2014. Two years of free credit monitoring will be offered to affected members. Should you have any questions or need additional information, please contact Daniel Dilley, Executive Director, Insurance Compliance by e-mail at Daniel.Dilley@usaa.com or by phone at (210) 913-0253.

Thank you,

Dana Simmons
Executive Vice President, Chief Administrative Officer
USAA

5246

9800 Fredericksburg
San Antonio, Texas 78288

Name
Address
City, State Zip

Month Day Year

Reference: Your usaa.com Information

Dear Name,

USAA takes the protection of our members' personal information very seriously, so we are writing to inform you about a recent incident that may have involved your information. During the morning of July 26, 2014, a technical error occurred and another USAA member may have viewed your personal information when logged onto the USAA mobile app or usaa.com. We immediately corrected the technical error and are examining measures we can take to help prevent similar incidents in the future.

Information That May Have Been Viewed
The personal information involved in this incident may have included your first and last name, address, checking and savings account numbers and transactions, loan balances and general information, insurance policies, Social Security number (on certain USAA Online Documents) and other general information available through usaa.com and USAA's mobile app.

Please Accept Our Apology
We deeply regret that this incident occurred and take the privacy and security of your personal information very seriously. Although we have no reason to believe your personal information has been misused, we recommend you closely review the enclosed information for steps you may take to protect your personal information.

Complimentary Credit Monitoring
As a precaution and to help protect your identity, we are offering a complimentary two-year membership of Experian's® ProtectMyID® Alert. 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. Please see the additional information we've enclosed on how to sign up.

Again, we deeply regret any concerns or inconvenience this incident may cause you. If you suspect you have been the victim of identity theft, or if you have any further questions about this incident or the efforts USAA is undertaking on your behalf, please call us at 1-877-393-9625. As always, it's our honor to serve you.

Sincerely,

Dana A. Simmons
Executive Vice President and Chief Administrative Officer
USAA

Activate ProtectMyID® Alert Now in Three Easy Steps

1. ENSURE that you enroll by: Month, day, year (Your code will not work after this date.)
2. VISIT the ProtectMyID® Alert website to enroll: www.protectmyid.com/redeem
3. PROVIDE your Activation Code: CODE (a credit card is not required for enrollment.)

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement # engagement number.

Additional Details Regarding Your Two-Year ProtectMyID® Alert Membership

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

- Free copy of your Experian credit report
- 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 ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID® Alert membership has expired.
- $1 Million Identity Theft Insurance[1]: Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID® Alert is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID® Alert, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902.

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates 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.

128851-XXXX

Steps to Take to Protect Your Personal Information

Always remain vigilant for signs of fraud or identity theft, and consider taking one or more of the below steps to protect your personal information. You can also obtain information from the below sources about fraud alerts and security freezes.

- Carefully examine all account transactions, statements and free credit reports to verify transactions. If anything looks suspicious or unusual, or if you believe you are the victim of identity theft, promptly report it to USAA and your other financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft.

- The FTC offers consumer assistance relating to identity theft, fraud alerts and security freezes. You may wish to visit the FTC web site at *www.ftc.gov/idtheft*, call the FTC's toll-free number at 1-877-438-4338, or contact them by mail at 600 Pennsylvania Ave., NW, Washington, DC 20580, to obtain further guidance or report suspected identity theft.

- You may also periodically obtain credit reports from each nationwide credit reporting agency: Equifax, Experian or Transunion. Under federal law, you are entitled to one free copy of your credit report every 12 months from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. You may request a free copy of your credit report by going to *www.annualcreditreport.com*, or by contacting one of the three nationwide consumer reporting at:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	*www.experian.com*	*www.transunion.com*

- You may also request that a fraud alert be placed on your credit file. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. To place a fraud alert, contact the fraud department of one of the three nationwide credit reporting agencies listed above (Equifax, Experian or TransUnion). When you request a fraud alert from one agency, it will notify the other two for you. You can place an initial fraud alert for 90 days and cancel fraud alerts at any time. During this process, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number.

- In addition, you can contact the three nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization. A security freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each nationwide credit reporting agency listed above (Equifax,

Experian or TransUnion) by sending a written request by regular, certified or overnight mail.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); complete address; social security number; and date of birth;
2. If you have moved in the past five (5) years, you may also need to provide the addresses where you have lived over the prior five years;
3. You may also need to provide two forms of identification (such as utility bill, pay stub with address or telephone bill) to verify your address.
4. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
5. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
6. If you are not a victim of identity theft, fees for security freezes may apply. Include payment by check, money order, or credit card. Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

Additional Information for Residents of Iowa:

- You may contact local law enforcement or the Iowa Attorney General's Office to report suspected identity theft. You can contact the Iowa Attorney General at: visit www.iowaattorneygeneral.gov; call 515-281-5264, or by mail at 1305 E. Walnut Street, Des Moines, IA 50319.

Additional Information for Residents of Maryland:

- You may obtain information about avoiding identity theft from the FTC (contact information listed above) or the Maryland Attorney General's Office. You can contact the Maryland Attorney General's Office at: visit www.oag.state.md.us, call toll-free at 1-888-743-0023, or by mail at Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202.

Additional Information for Residents of North Carolina:

- You may obtain information about avoiding identify theft from the FTC (contact information listed above) or the North Carolina Attorney General's Office. You can contact the North Carolina Attorney General at: visit www.ncdoj.gov, call toll-free at 1-877-566-7226, or by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001.