

STATE OF NH
DEPT OF JUSTICE
2015 JUL 31 AM 11:37



Woodbury Financial Services, Inc. | Member FINRA, SIPC, and Registered Investment Adviser
P.O. Box 64284, St. Paul, MN 55164 | (800) 800-2638 | woodburyfinancial.com

July 27, 2015

Mr. Joseph Foster, Attorney General
NH Department of Justice
33 Capitol St
Concord, NH 03301

RE: Notification of Privacy Risk Incident

Dear Attorney General Foster:

Pursuant to New Hampshire Rev. Stat. § 359-C:20, please allow this letter to serve as Woodbury Financial Services, Inc.'s ("Woodbury") official notification to the New Hampshire Attorney General that a privacy risk incident was recently identified.

On May 28, 2015, a Woodbury Registered Representative's laptop computer was accessed by an unauthorized individual as part of a phishing scam. The laptop computer contained spreadsheets that included information belonging to New Hampshire residents. It cannot be confirmed if the information was accessed or viewed by the unauthorized individual. The laptop computer was scanned, cleaned and deemed free of viruses. The information contained the New Hampshire residents' names, Social Security numbers and/or driver's license numbers.

The Company provided written notice to three New Hampshire residents on July 24, 2015 including 24 months of credit monitoring and identity theft protection paid for by our Company. A copy of this notification is included.

If you have any questions, please feel free to contact me directly.

Yours,

Sarah Canaday
Senior Compliance Specialist
Woodbury Financial Services, Inc.
Phone: 651-702-1866
Sarah.canaday@woodburyfinancial.com

[DATE]

[NAME]

[ADDRESS]

[ADDRESS]

Dear [NAME]:

We are writing to inform you of a potential unauthorized acquisition of your personal information that occurred on May 28, 2015. A Woodbury Financial Services Registered Representative's laptop computer was accessed by an unauthorized individual as part of a phishing scam. He had documents containing your name, Social Security number and/or driver's license number stored on his computer.

Although we have no evidence that your information was in fact accessed by the unauthorized individual or that your information has been or will be misused, as a precaution we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this letter and you can use them at any time during the next 24 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. You are automatically eligible to use this service – there is no action required on your part. If a problem arises, simply call 866-979-2595 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling **866-979-2595** using the following redemption code: XXXXXXXX. (Please note: additional steps may be required by you in order to activate your phone alerts.)

There are other steps you can take to further protect yourself against identity theft or other unauthorized use of personal information if you are concerned. Information regarding these steps is provided on the following pages.

We apologize for any inconvenience or concern that this matter may cause you. We remain committed to protecting the privacy of your personal information. If I may be of further assistance, please feel free to contact me directly.

Sincerely,

Sarah Canaday
Woodbury Financial Services
Privacy Specialist
Direct: (651) 702-1866

Enclosures

Steps You May Take To Protect Yourself Against Potential Misuse of Information

You can take some simple steps to protect yourself against possible identity theft or other fraudulent misuse of your information.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**
As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or suspected incidence of identity theft to proper law enforcement authorities or the Federal Trade Commission (FTC).

To file a complaint with the FTC, you may do so at www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). The FTC mailing address is 600 Pennsylvania Ave. NW, Washington, DC 20580. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Copy of Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies is provided below:

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	Transunion (800) 888-4213 www.transunion.com P.O. Box 1000 Chester, PA 19022
--	--	--

- **Fraud Alerts and Security Freezes**

In addition, you may contact the fraud departments of the three national consumer reporting agencies or the FTC to obtain information about placing fraud alerts or security freezes in your file. You have the right to ask that the three credit reporting companies place fraud alerts in your 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. However, it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three national credit reporting companies. As soon as that company processes your fraud alert, it will notify the other two credit reporting companies which then

must also place fraud alerts in your file. In addition, you can contact the national credit reporting agencies regarding if and how you may place a security freeze on your credit report. 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 credit reporting agency.

Please see the above table for contact information for the three national consumer reporting agencies.

- **Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit <http://www.consumer.ftc.gov/topics/privacy-identity> or call 1-877-ID THEFT (877-438-4338).

Terms of Use for AllClear Secure

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- Automatic 12 months of coverage;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services (“Services”) to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

You are automatically protected for 12 months from the date the breach incident occurred, as communicated in the breach notification letter you received from Company (the “Coverage Period”). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements

To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen eighteen (18) years of age or older, reside in the United States, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8075 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Secure Does Not Apply to the Following:

Any expense, damage or loss:

- Due to

- Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
- Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your “Misrepresentation”)
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur;
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud; and
- You are expected to protect your personal information in a reasonable way at all times. Accordingly, you will not recklessly disclose or publish your Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information, such as, by way of example, in response to “phishing” scams, unsolicited emails, or pop-up messages seeking disclosure of personal information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

<p><u>E-mail</u> support@allclearid.com</p>	<p><u>Mail</u> AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701</p>	<p><u>Phone</u> 1.855.434.8077</p>
--	---	---