

February 10, 2017

Consumer Protection and Antitrust Bureau  
Office of the Attorney General of New Hampshire  
33 Capitol Street  
Concord, NH 03301

Re: Notification of a Breach of Security

Dear Attorney General Foster,

On February 1, 2017, one of our employees emailed the IRS Form W-2 information of one (1) current or former New Hampshire employee in response to what they later learned was a fraudulent email purporting to be from our CEO requesting the information. In fact, the email was a phishing email that came from an external email address. The W-2 information included the employee's social security number, 2016 wage information, and current mailing address.

We learned of the incident that same day and immediately investigated. We have filed a police report, notified the FBI, contacted the IRS to notify them of the incident and are in the process of contacting the affected state revenue agencies. As of the date of this letter, we have no evidence that any of the information has been misused.

We emailed the impacted employee on February 2 to alert the employee that the incident occurred and have been in regular communication with the employee since that time. We prepared the attached notification letter to comply with New Hampshire law and are sending this notice to the impacted employee contemporaneously with this letter. As the attached letter explains, we are offering 24 months of credit monitoring and fraud remediation services through AllClear ID.

We take the privacy and security of our employees' information very seriously. If you have any questions about this incident, please contact me at 617-715-7795.

Sincerely,



Jonathan Poole  
Chief Financial Officer

STATE OF NH  
DEPT OF JUSTICE  
2017 FEB 24 AM 11:50

STATE OF NH  
DEPT OF JUSTICE  
2017 FEB 24 AM 11:50

**February 10, 2017**

[Name]

[Address]

[City], [State] [ZIP]

Dear [Name],

As you know, there was a recent breach of security involving your IRS Form W-2 information.

**Why you are receiving this notice:** The law of your state of residence requires that we notify you of the incident by mail to your last known address.

**What happened:** As you know, on February 1, 2017, one of our employees emailed W-2 information in response to what they later learned was a fraudulent email purporting to be from our CEO. In fact, the email was a phishing email that came from an external email address.

**What information was involved:** The incident involved your IRS Form W-2, which included your social security number, 2016 wage information, and mailing address.

**What are we doing:** We filed a police report, are cooperating with law enforcement, and are in communication with the IRS and state revenue agencies. We are taking appropriate steps to address the incident and are committed to protecting your information.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. These services are being offered to comply with certain state legal requirements and, as a result, are being extended to employees who live in states without such requirements entirely as a courtesy in order to treat our employees equally. The offer therefore is not intended and should not be taken to suggest or acknowledge that recipients of the offer are at any substantial risk of harm.

The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months. The terms and conditions of the services are attached to this letter.

**AllClear Identity Repair:** This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-866-979-2595 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

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

**What you can do:** Attached to this letter is additional information about Identity Theft Protection. If you have further questions or concerns about this incident, please contact me ([jonathan.poole@genocsea.com](mailto:jonathan.poole@genocsea.com)) or Tom Bures ([tom.bures@genocsea.com](mailto:tom.bures@genocsea.com)) or call us at 617-715-7795.

We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

A handwritten signature in black ink, appearing to be 'JP' or 'Jonathan Poole'.

Jonathan Poole  
Chief Financial Officer



**Information about Identity Theft Prevention**

We recommend that, as a consumer, you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

**Equifax**, P.O. Box 105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, [www.equifax.com](http://www.equifax.com)

**Experian**, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com)

**TransUnion**, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, [www.transunion.com](http://www.transunion.com)

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Consumers should always remain vigilant with respect to reviewing their account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, a state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

**Federal Trade Commission**, Consumer Response Center

600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**For residents of Maryland:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

**Maryland Office of the Attorney General**, Consumer Protection Division

200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us)

**For residents of Massachusetts:** You also have the right to obtain a police report.

**For residents of North Carolina:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

**North Carolina Attorney General's Office**, Consumer Protection Division

9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, [www.ncdoj.gov](http://www.ncdoj.gov)

**For residents of Rhode Island:** You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office:

**Rhode Island Attorney General's Office**, Consumer Protection Division

150 South Main Street, Providence, RI 02903 (401) 274-4400,

<http://www.riag.ri.gov/ConsumerProtection/About.php#>



**Fraud Alerts:** There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, [www.equifax.com](http://www.equifax.com)  
Experian: 1-888-397-3742, [www.experian.com](http://www.experian.com)  
TransUnion: 1-800-680-7289, [www.transunion.com](http://www.transunion.com)

**Credit Freezes (for Non-Massachusetts Residents):** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax, P.O. Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)  
Experian, P.O. Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, [www.transunion.com](http://www.transunion.com)

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

**Credit Freezes (for Massachusetts Residents):** Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax, P.O. Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)  
Experian, P.O. Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, [www.transunion.com](http://www.transunion.com)

*Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible,

display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.



### **AllClear Identity Repair Terms of Use**

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:

- 24 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair 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 Identity Repair 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**

Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the “Coverage Period”). Fraud Events (each, an “Event”) that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

#### **Eligibility Requirements**

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, 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 Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair 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; and
- 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 Identity Repair 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, or
  - 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; or

- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair 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 Identity Repair 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.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

**Opt-out Policy**

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

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