



Sean B. Hoar
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

February 15, 2017

File No. 36974.03

VIA E-MAIL

Attorney General Joseph Foster
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
E-Mail: attorneygeneral@doj.nh.gov

Re: Data Security Incident

Dear Attorney General Foster:

I represent Goode Compliance International (GCI), located in Miramar, Florida. This letter is being sent pursuant to N.H. Rev. Stat §§ 359-C:19-359-C:21 because GCI learned on January 26th, 2017, that the personal information of one (1) resident of New Hampshire may have been involved in a data security incident. The information included names, addresses, Social Security numbers, and tax and wage information.

The incident occurred on January 25th, 2017, and affected GCI employee Form W-2 Wage and Tax Statement information. Immediately upon discovering the incident, GCI notified the Internal Revenue e-File Services Department and the Internal Revenue Service/Criminal Investigation (IRS/CI) to prevent fraudulent activity. GCI also immediately notified its employees of the incident, including the affected New Hampshire resident, with the attached emails. It also followed up with the attached letter. As referenced in the letter, GCI will provide 12 months of credit monitoring and identity protection services to the affected New Hampshire resident through ID Experts. Please contact me should you have any questions.

Sincerely,

A handwritten signature in blue ink that reads 'Sean B Hoar'.

SEAN B. HOAR of
LEWIS BRISBOIS BISGAARD & SMITH LLP

cc. Jeremy Cortese, Vice President Operations
Goode Compliance International



<<Date>>

<<Employee First Name>> <<Employee Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Subject: Data Security Incident

Dear <<Employee First Name>> <<Employee Last Name>>:

I am writing to inform you of a data security incident that involved your personal information. We take the privacy and security of your information very seriously. This is why we are contacting you, offering you credit monitoring services, and informing you about steps that can be taken to protect your personal information.

What Happened? On January 26, 2017, we discovered that Form W-2 Wage and Tax Statement information for certain employees may have been accessed without authorization on January 25, 2017. As soon as we discovered the incident, we notified the Internal Revenue e-File Services Department and the Internal Revenue Service/Criminal Investigation (IRS/CI) in order to prevent fraudulent activity.

What Information Was Involved? The information involved Form W-2 Wage and Tax Statement information which included names, addresses, Social Security numbers, and tax and wage information.

What Are We Doing? As soon as we discovered the incident, we took the steps discussed above. We will provide the IRS/CI whatever cooperation is necessary to hold the perpetrators accountable. We are also providing you information about steps you can take to protect your personal information, and are offering you credit and identity monitoring services for 12 months at no cost to you through ID Experts®. Those services, called MyIDCare™, include 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. We are also enhancing the security of how we handle W-2 information, making it more difficult for similar incidents to occur in the future.

What You Can Do: You can follow the recommendations on the following page to protect your personal information. You can also contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to www.idexpertscorp.com/protect and using the Access Code which will be provided to you directly by (insert name or title of GCI employee who will provide the codes on Monday to employees) on Monday, January 30, 2017. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. Please note the deadline to enroll is April 30, 2017. To receive credit services, you must be over the age of 18

and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Your services start on the date you enroll in the services and can be used at any time thereafter for 12 months from the date of this notice.

For More Information: Further information about how to protect your personal information appears on the following page. You can also call Devon Rivera of Goode Compliance, at 954-399-7510 ext. 316.

If you haven't already done so, we also encourage you to complete IRS Form 14039, Identity Theft Affidavit which you can obtain at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>, and then mail or fax it to the IRS according to instructions on the form. If you have other identity theft/tax related issues, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

<<Signature>>

Jeremy Cortese

Vice President Operations

STEPS YOU CAN TAKE TO FURTHER PROTECT 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 any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

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 <http://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 this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: In some US states, you have the right to put a security freeze on your credit file. This 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 credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
401-274-4400