



Attorneys at Law

JOSEPH J. LAZZAROTTI
DIRECT DIAL: (973) 451-6363
EMAIL: LAZZAROTTIJ@JACKSONLEWIS.COM

Jackson Lewis P.C.
220 Headquarters Plaza
East Tower, 7th Floor
Morristown, NJ 07960-6834
Tel 973 538-6890
Fax 973 540-9015
www.jacksonlewis.com

Richard J. Cino - Managing Principal

Representing Management Exclusively in Workplace Law and Related Litigation

- ALBANY, NY ALBUQUERQUE, NM ATLANTA, GA AUSTIN, TX BALTIMORE, MD BIRMINGHAM, AL BOSTON, MA CHICAGO, IL CINCINNATI, OH CLEVELAND, OH DALLAS, TX DAYTON, OH DENVER, CO DETROIT, MI GRAND RAPIDS, MI GREENVILLE, SC HARTFORD, CT HONOLULU, HI HOUSTON, TX INDIANAPOLIS, IN JACKSONVILLE, FL KANSAS CITY REGION LAS VEGAS, NV LONG ISLAND, NY LOS ANGELES, CA MADISON, WI MEMPHIS, TN MIAMI, FL MILWAUKEE, WI MINNEAPOLIS, MN MONMOUTH COUNTY, NJ MORRISTOWN, NJ NEW ORLEANS, LA NEW YORK, NY NORFOLK, VA OMAHA, NE ORANGE COUNTY, CA ORLANDO, FL PHILADELPHIA, PA PHOENIX, AZ PITTSBURGH, PA PORTLAND, OR PORTSMOUTH, NH PROVIDENCE, RI RALEIGH, NC RAPID CITY, SD RICHMOND, VA SACRAMENTO, CA SALT LAKE CITY, UT SAN DIEGO, CA SAN FRANCISCO, CA SAN JUAN, PR SEATTLE, WA ST. LOUIS, MO TAMPA, FL WASHINGTON, DC REGION WHITE PLAINS, NY

\*through an affiliation with Jackson Lewis P.C., a Law Corporation

March 29, 2017

VIA OVERNIGHT MAIL

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Breach Notification

Dear Attorney General:

On behalf of our client, Glenn R. Millar, CPA, PC (the "Company"), we are writing to notify you of a breach of security of personal information involving two (2) New Hampshire residents.

On October 12, 2016, the Company discovered that it was victimized by a hacking into its information systems that occurred sometime between May and July 2016. Based on its investigation, which included a forensic review of its systems by a nationally recognized third-party forensic investigation firm, the Company determined that approximately 404 individuals had been affected, with none of those being New Hampshire residents. The Company notified those individuals about the incident on or about November 18, 2016.

On or about March 9, 2017, despite the extensive forensic analysis of its systems in connection with initial discovery by a nationally recognized forensic investigation firm, the Company discovered that 909 additional individuals were affected by the incident, including two residents of New Hampshire. These individuals will be notified this week and a draft copy of the notification is attached.

As set forth in the attached letter, the Company has taken numerous steps to protect the security of the personal information of the affected individuals. Immediately upon discovering the incident, in addition to working with the forensic services provider referred to above, the Company contacted various law enforcement agencies including the Internal Revenue

1 Please note that by providing this letter the Company is not agreeing to the jurisdiction of the State of New Hampshire, or waiving its right to challenge jurisdiction in any subsequent actions.

Service. The Company also changed system passwords, including for its accounting and tax software products, among other measures. Also, in addition to continuing to monitor this situation, the Company is reexamining its current data privacy and security policies and procedures to find ways of reducing the risk of future data incidents. Should the Company become aware of any significant developments concerning this situation, we will inform you.

If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS P.C.



Joseph J. Lazzarotti

Encl.

4825-0676-0005, v. 1



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name>>  
<<Address1>>  
<<Address2>>  
<<City>><<State>><<Zip>>

<<Date>>

### **Notice of Data Breach**

Dear <<Name>>

Our firm (the "Firm") discovered on or about March 9, 2017, that a data security incident that we initially discovered during October 2016 affected more individuals than our initial investigation showed. The incident involves some of our clients and their spouses and dependents, where applicable. We are sending this advisory to you so that you can take steps to protect yourself and minimize the possibility of misuse of your information. We sincerely apologize for any inconvenience this may cause you and assure you that we have and continue to deploy measures to avoid these kinds of incidents from happening.

#### **What Happened**

Based on our investigation to date, we believe unauthorized persons hacked into our information systems between the period of May to July 2016, and used data on the system to fraudulently file federal income tax returns. On or about March 9, 2017, we discovered this incident may also affect you.

#### **What Information Was Involved**

The personal information that may have been acquired includes name, birth date, telephone number(s), address, social security number, financial account information, and bank account information including account number and routing information.

#### **What We Are Doing to Protect You**

When we initially discovered the incident, we immediately began an investigation and contacted various federal and state agencies and law enforcement including the Internal Revenue Service. We have updated our accounts with the IRS and our tax preparation software vendor. We also engaged a third party IT forensics firm to assist us with our investigation and remediation. Based on our initial investigation, we believed that the incident affected only certain clients and we have notified them. Upon discovering more clients affected by the incident on March 9, 2017, we again took steps to ensure our systems were secured and updated the IRS. This notification has not been delayed as a result of any law enforcement investigation.

We have arranged for Equifax to provide its Credit Watch Silver identity theft protection product for one year at no cost to you. If you choose to take advantage of this product, it will provide you with a notification of any changes to your credit information and access to your credit report. A description of this product is provided in the attached material. You must complete the enrollment process no later than 60 days from the date of this letter. We urge you to consider enrolling in this product at our expense.

**What You Can Do**

The attached sheet describes steps you can take to protect your identity, credit and personal information, including enrolling in the credit monitoring services being provided at no cost to you.

**For More Information**

Again, we apologize for this situation. We treat all client information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. Theft of data and similar incidents are difficult to prevent in all instances, however, we will be reviewing our systems and making improvements where we can to minimize the chances of this happening again.

If you have questions you should call 1-844-469-3935.

Sincerely,



Glenn Millar, CPA  
(623) 878-4111

**PLEASE SEE ATTACHED FOR ADDITIONAL INFORMATION**

## What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:
  - Add a fraud alert statement or security freeze to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
  - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
  - Obtain a free copy of your credit report by going to [www.annualcreditreport.com](http://www.annualcreditreport.com).

Equifax  
P.O. Box 740256  
Atlanta, GA 30374  
(800) 525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 9554  
Allen, TX 75013  
(888) 397-3742  
[www.experian.com/consumer](http://www.experian.com/consumer)

TransUnion  
P.O. Box 2000  
Chester, PA 19022  
(800) 888-4213  
[www.transunion.com](http://www.transunion.com)

2. Please review all bills and credit card statements closely to determine whether you have been charged for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes delay their use of stolen personal information.
3. The Federal Trade Commission (“FTC”) offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You can also obtain information from the FTC about fraud alerts and security freezes. You may contact the FTC by visiting [www.ftc.gov](http://www.ftc.gov) or [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), calling (877) 438-4338, or writing to the FTC at the address below. If you suspect or know that you are the victim of identity theft, you should contact local police. You can also report such activity to the Fraud Department of the FTC, which will collect all relevant information and make it available to law-enforcement agencies. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.
4. **Oregon Residents:** To obtain additional information about avoiding identity theft, you may contact the Oregon Attorney General’s Office, using the contact information below:

Oregon Department of Justice  
1162 Court Street NE  
Salem, OR 97301-4096  
Phone: (503) 378-4400

## About the Equifax Credit Watch™ Silver identity theft protection product

Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file. Note: You must be over age 18 with a credit file in order to take advantage of the product.

Equifax Credit Watch provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax** credit report
- Wireless alerts and customizable alerts available (available online only)
- One copy of your Equifax Credit Report™
- Up to \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m. to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance, and help initiate an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality (available online only)

**How to Enroll:** To sign up online for **online delivery** go to: [www.myservices.equifax.com/silver](http://www.myservices.equifax.com/silver)

1. **Welcome Page:** Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
2. **Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.