

Representing Management Exclusively in Workplace Law and Related Litigation

**jackson lewis**  
Attorneys at Law

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 Shareholder

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

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

March 16, 2017

**VIA OVERNIGHT MAIL**  
Office of the Attorney General  
33 Capital Street  
Concord, NH 03301

STATE OF NH  
DEPT OF JUSTICE  
2017 MAR 17 AM 10:54

Re: **Data Incident Notification**<sup>1</sup>

Dear Sir/Madam:

Please be advised that on February 20, 2017, our client, Bacon & Company CPAs, LLC ("Bacon & Company") discovered a data security incident which resulted in unauthorized access to data files which may have contained personal information of Bacon & Company clients including name, address, birth date, Social Security number, and financial account information.

Immediately upon discovering the intrusion, Bacon & Company commenced an investigation to determine the scope of this incident and identify those affected. Bacon & Company worked with its information technology team to conduct a thorough scan of its computer information systems in an effort to ensure the attack did not result in any additional exposure to personal information and took steps to confirm the integrity of Bacon & Company's computer information systems. It appears that 1,157 individuals could have been affected, including 8 residents of New Hampshire. Based on the investigation to date, Bacon & Company believes an unauthorized person(s) hacked into its computer information system and used data on the system to fraudulently file income tax returns. In light of this incident, Bacon & Company plans to begin notifying the affected individuals in the next several days. A draft copy of the notification that will be sent is attached.

As set forth in the attached letter, Bacon & Company has taken numerous steps to protect the security of the personal information of the affected individuals. In addition to this notice, Bacon & Company has filed a complaint with the Internet Crime Complaint Center which is co-sponsored by the Federal Bureau of Investigation ("FBI") and the National White Collar Crime Center and notified the Rhode Island State Police of the incident. Bacon & Company also filed a report with the Warwick Police Department. Additionally, Bacon & Company has notified the Rhode Island Division of Taxation and the Internal Revenue Service ("IRS") of this incident and is currently working with its IRS Stakeholder Liaison. Further, Bacon & Company notified the Rhode Island Attorney General. Also, in addition to continuing to monitor this situation, Bacon & Company is reexamining its current data privacy and security policies and procedures to find ways of reducing the risk of future data incidents. Should Bacon & Company become aware of any significant

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

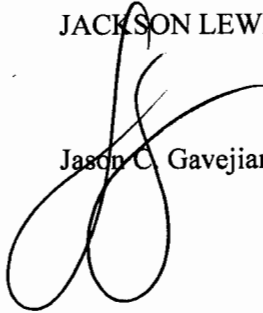
developments concerning this situation, we will inform you.

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

Sincerely,

JACKSON LEWIS P.C.

Jasop C. Gavejian

A handwritten signature in black ink, appearing to read 'Jasop C. Gavejian', is written over the typed name. The signature is stylized with large loops and a long horizontal stroke extending to the right.

Enclosure

4849-4378-8612, v. 1

**[[COMPANY]]  
LETTERHEAD]**

**[Insert name]**  
**[Insert address]**

Dear **[Insert name]**,

On February 20, 2017, Bacon & Company CPAs, LLC ("Bacon & Company") discovered a data security incident which resulted in unauthorized access to data files which may have contained your personal information including name, address, birth date, Social Security number, and financial account information. 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 apologize for any inconvenience this may cause you and assure you we are working diligently to resolve this incident.

Immediately upon discovering the intrusion, we commenced an investigation to determine the scope of this incident and identify those affected. We worked with our information technology team to conduct a thorough scan of our computer information systems in an effort to ensure the attack did not result in any additional exposure to personal information and took steps to confirm the integrity of Bacon & Company's computer information systems. We have also filed a complaint with the Internet Crime Complaint Center which is co-sponsored by the Federal Bureau of Investigation ("FBI") and the National White Collar Crime Center. We have notified the Rhode Island State Police of the incident and filed a police report with the Warwick Police Department. Additionally, we have notified the Rhode Island Division of Taxation and the Internal Revenue Service ("IRS") of this incident and are currently working with our IRS Stakeholder Liaison. Further, we have also notified the Rhode Island Attorney General. Based on our investigation to date, we believe unauthorized person(s) hacked into our computer information system and used data on the system to fraudulently file income tax returns. Notwithstanding these steps, set forth below are additional steps you can take to protect your identity, credit, and personal information.

As an added precaution we have arranged for Equifax Personal Solutions to help protect your identity and your credit information by providing you with 12 months of Equifax Credit Watch Silver identity theft protection at no cost to you. **To receive these services you must enroll with Equifax Credit Watch within 60 days of the date of this letter.** You may contact Equifax Credit Watch immediately for purposes of (i) enrolling in the program, (ii) assisting you in learning more about identity theft solutions, and (iii) answering some of your questions regarding the incident.

Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring of your Equifax credit report with daily notification of key changes to your credit file.
- Wireless alerts and customizable alerts available.
- One copy of your Equifax Credit Report.
- \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you.
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality

**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 your letter 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.

We treat all sensitive 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 or concerns you should call [Insert Number] from 6:00 am to 6:00 pm Pacific Time, Monday through Friday. Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

[Insert name and title]

#### **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. Contacting the nationwide credit-reporting agencies as soon as possible to:
  - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a 90 day fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert tab, visit [www.fraudalerts.equifax.com](http://www.fraudalerts.equifax.com) or call our auto fraud line at 1-877-478-7625, and follow the simple prompts. 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.
  - Receive 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. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive 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 hold on to stolen personal information before using it.
3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues and how to avoid identity theft. The FTC can be contacted either by visiting [www.ftc.gov](http://www.ftc.gov), [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local police and you also can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue

NW Washington, DC 20580

4. The IRS also offers Identity Protection: Prevention, Detection and Victim Assistance which can be found at: <https://www.irs.gov/Individuals/Identity-Protection>.
5. If you believe you are a victim of identity theft you should immediately report same to law enforcement.
6. For *North Carolina Residents*: For more information on identity theft please contact either the Federal Trade Commission at the contact information provided above, or North Carolina's Attorney General's Office, Address: 9001 Mail Service Center, Raleigh, NC 27699-9001; Telephone: (919) 716-6400; Fax: (919) 716-6750; website: [www.ncdoj.com/](http://www.ncdoj.com/)

4842-1352-1220, v. 1