

RECEIVED

MAY 23 2017

BakerHostetler

CONSUMER PROTECTION

Baker & Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Eric A. Packel
direct dial: 215.564.3031
epackel@bakerlaw.com

May 18, 2017

VIA OVERNIGHT MAIL

Joseph Foster
Office of the Attorney General
33 Capitol St
Concord, NH 03301

Re: *Incident Notification*

Dear Attorney General Foster:

We are writing on behalf of our client, Ricoh USA, Inc. ("Ricoh"), to notify you of a security incident involving a New Hampshire resident.

On April 20, 2017, Equifax Workforce Solutions ("Equifax"), which provides payroll-related services to Ricoh, informed Ricoh that it had been investigating potential unauthorized access to Equifax's systems. The investigation determined that an unauthorized individual(s) may have accessed some of Ricoh's current and former employees' payroll information through Equifax's systems. Please note that this incident occurred at Equifax, and Ricoh's own systems were **not** compromised.

Equifax informed Ricoh that the unauthorized individual may have accessed an electronic copy of some of Ricoh's current and former employees' 2016 W-2s, which includes names, addresses, Social Security numbers, and, to the extent that some employees' Equifax account contains any banking information, that information may also be affected. This incident did not affect all of Ricoh's current and former employees.

Ricoh is notifying 1 New Hampshire resident in substantially the same form as the letter attached hereto, with written notification commencing May 18, 2017.¹ Ricoh is offering affected individuals a complimentary three-year membership of credit monitoring and identity theft protection through Equifax's® ID Patrol. Notification is being provided in the most expedient

¹ This report is not, and does not constitute, a waiver of personal jurisdiction.

Joseph Foster
May 18, 2017
Page 2

time possible pursuant to the investigation described above, which was necessary to determine the scope of the incident; restore the reasonable integrity of the data system; and identify the individuals potentially affected. See N.H. Rev. Stat. § 359-C:20(I)(a).

To help prevent a similar incident from happening in the future, Ricoh is working with Equifax on implementation of additional security measures for their systems.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in cursive script, appearing to read "Eric A. Packel".

Eric A. Packel

Enclosure



Ricoh USA, Inc.
70 Valley Stream Parkway
Malvern, PA 19355

May 18, 2017

[ADDRESS BLOCK]

Dear [EMPLOYEE NAME]:

Ricoh is committed to protecting the confidentiality and security of our employees' personal information. Regrettably, this notice concerns an incident involving some of that information. If you are a current employee, you were also sent an email notification regarding this incident on May 3, 2017.

On April 20, 2017, Equifax Workforce Solutions ("Equifax"), which provides payroll-related services to Ricoh, informed us that it had been investigating potential unauthorized access to its systems. The investigation determined that an unauthorized individual(s) may have accessed some of our current and former employees' payroll information through Equifax's systems. Equifax informed us that the unauthorized individual may have accessed an electronic copy of some of our current and former employees' 2016 W-2s, including your W-2. The information on the W-2 form includes your name, address, and Social Security number. To the extent your Equifax account contains any of your banking information, that information may also be affected. Please note that this incident occurred at Equifax, and Ricoh's own systems were **not** compromised. This incident did not affect all of our current and former employees.

We are notifying you out of an abundance of caution so that you can take appropriate steps to protect yourself and to offer you a complimentary three-year membership of Equifax's® ID Patrol. ID Patrol will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies. **For more information on Equifax's® ID Patrol, including instructions on how to activate your complimentary three-year membership, as well as some additional steps you can take to protect yourself, please see the page that follows this letter.**

We sincerely regret any inconvenience this may cause you. To help prevent a similar incident from happening in the future, we are working with Equifax on implementation of additional security measures for their systems. If you have any questions, please call 1-800-256-4094 or email PayrollHotline@ricoh-usa.com.

Sincerely,

Ricoh Payroll Department

**ADDITIONAL DETAILS REGARDING YOUR 36-MONTH
EQUIFAX® ID PATROL MEMBERSHIP**

- Visit www.myservices.equifax.com/patrol for more information and to enroll for ID Patrol.
- Your activation code is [INDIVIDUAL CODE] and is valid for the next 90 days and is non-transferable.

ENROLLMENT TIPS:

1. Use the link above to access your custom ID Patrol Enrollment page (**your activation code will NOT work if you use a different link**).
2. Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
3. The platform will walk you through the enrollment, enter the information requested and click the Continue button to step through the account setup screens.
4. 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. You will see an order confirmation page and you can click View My Product to access the product features.
6. You will receive a confirmation email.

Coverage under ID Patrol will expire 36 months from the date you activate your code by enrolling for ID Patrol online.

ID Patrol provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your Equifax, Experian, and TransUnion credit reports.
- Wireless alerts and customizable alerts available.
- One 3-in-1 Credit Report and access to your Equifax Credit Report™.
- Ability to receive alerts if your Social Security Number or credit card numbers are found on Internet trading sites (available online only).
- Ability to lock and unlock your Equifax Credit Report.
- Up to \$1 million in identity theft insurance with \$0 deductible.

Once enrolled, your ID Patrol comes with 24/7 live agent Customer Service 1-877-474-8273 to assist you in understanding the content of your Equifax credit information, provide personalized identity theft victim assistance and when initiating an investigation of inaccurate information

Additional Steps You Can Take

Even if you choose not to take advantage of this free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or

call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you know or suspect you are a victim of tax-related identity theft, the IRS recommends these steps:

- Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.
- Complete IRS Form 14039, Identity Theft Affidavit, if your efiled return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.

If you previously contacted the IRS and did not have a resolution, contact the IRS for specialized assistance at 1-800-908-4490.