

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

**From:** Moore, Desiree F. <[Desiree.Moore@klgates.com](mailto:Desiree.Moore@klgates.com)>  
**Sent:** Thursday, December 3, 2020 7:44 PM  
**To:** DOJ: Attorney General <[attorneygeneral@doj.nh.gov](mailto:attorneygeneral@doj.nh.gov)>  
**Subject:** Notice of Security Incident

**EXTERNAL:** Do not open attachments or click on links unless you recognize and trust the sender.

---

To whom it may concern:

Kindly note that I am legal counsel for USNR LLC (“USNR”). I write regarding a recent data security incident at USNR.

On or about October 25, 2020, USNR detected that its systems were encrypted. Upon a thorough investigation, USNR determined that the individuals behind the encryption hacked into their system some weeks prior (unbeknownst to USNR) and, as a result, may have accessed select personal information relating to USNR employees, including one (1) New Hampshire resident. USNR internal teams worked diligently with forensic consultants to restore and secure the impacted systems and are engaging in a detailed review of its cybersecurity policies and procedures.

A sample notification is attached. The data subject(s) will be notified on December 7, 2020.

If you have any questions or require any additional information, please do not hesitate to contact me directly. Thank you.

Best regards,

Desiree



**Desiree Moore**

Partner

K&L Gates LLP

[desiree.moore@klgates.com](mailto:desiree.moore@klgates.com)

70 W. Madison St.

Suite 3100

Chicago, IL 60602

Phone: [+1 312 781 6028](tel:+13127816028)

[www.klgates.com](http://www.klgates.com)



Chicago Daily Law Bulletin. CHICAGO LAWYER



This electronic message contains information from the law firm of K&L Gates LLP. The contents may be privileged and confidential and are intended for the use of the intended addressee(s) only. If you are not an intended addressee, note that any disclosure, copying, distribution, or use of the contents of this message is prohibited. If you have received this e-mail in error, please contact me at [Desiree.Moore@klgates.com](mailto:Desiree.Moore@klgates.com).



00549-FININS-AUTO

000001



USA

### Notice of Security Incident

Dear [REDACTED] :

We are writing to inform you about a data security incident that may have exposed some of your personal information. USNR takes the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

#### What happened?

On October 25, 2020, USNR, LLC (“USNR”) became aware of an intrusion into its data network that began on September 28, 2020. Specifically, unbeknownst to USNR, unknown individuals accessed USNR’s information systems and subsequently launched an attack designed to encrypt data files stored on its computer systems.

While the primary intent of the attack looks to have been to disrupt USNR’s operations, it appears that the intruders had the opportunity to access personal information relating to current and former USNR employees. This information potentially could have included: employee names, addresses, dates of birth, social security numbers, bank account information, and beneficiary information (including names, addresses, dates of birth, and social security numbers of beneficiaries). Please note that we have no evidence of such information being viewed, stolen, or otherwise misused as of the date of this letter.

#### What we are doing.

USNR is working with a leading third-party cybersecurity firm to rebuild its internal network and technology infrastructure, including securing all affected systems and engaging in a detailed review of its cybersecurity policies and procedures.

Additionally, to help relieve concerns and restore confidence following this incident, we have secured the services of Equifax to provide identity monitoring at no cost to you for one year. Equifax is a global leader in risk mitigation and response, and their team has extensive experience helping people who have potentially sustained an unintentional exposure of confidential data.

Additional information describing your services is included with this letter.

#### What you can do.

Please review the enclosed “Product Information” section included with this letter. This section describes the key features of the identity monitoring offering and how to enroll in identity monitoring. We have also included a resource guide with additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

#### For more information.

If you have questions, please call [hotline number], Monday through Friday from [REDACTED] to [REDACTED] Central Time.

Protecting your information is important to us. We trust that the steps we have taken and the services we are offering to you demonstrate our continued commitment to your security and well-being.

Sincerely,

Dale Brown  
President and CEO

## ADDITIONAL RESOURCES

**Contact information for the three nationwide credit reporting agencies is: Equifax, PO Box**

740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

**Experian, PO Box 2104, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742**

**TransUnion, PO Box 2000, Chester, PA 19022, [www.transunion.com](http://www.transunion.com), 1-800-888-4213**

**Free Credit Report.** It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit **[www.annualcreditreport.com](http://www.annualcreditreport.com)** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Fraud Alert.** You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

**Security Freeze.** You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

**Federal Trade Commission and State Attorneys General Offices.** 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-IDTHEFT (438-4338).

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), 1-877-566-7226.

**Reporting of identity theft and obtaining a police report.**

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.



Enter your Activation Code: XXXXXXXXXX

## Product Information

### **Equifax ID Patrol<sup>®</sup> provides you with the following key features:**

- 3-Bureau credit file monitoring<sup>1</sup> and alerts of key changes to your Equifax<sup>®</sup>, TransUnion<sup>®</sup> and Experian<sup>®</sup> credit reports
- Access to your Equifax credit report
- One Equifax 3-Bureau credit report
- Wireless alerts (available online only). Data charges may apply.
- Automatic Fraud Alerts<sup>2</sup>. With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit (available online only).
- Credit Report Lock<sup>3</sup> Allows users to limit access to their Equifax credit report by third parties, with certain exceptions.
- Internet Scanning<sup>4</sup> Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Lost Wallet Assistance. If you lose your wallet, we'll help you cancel and re-issue your cards and ID
- Up to \$1 MM in identity theft insurance<sup>5</sup>
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

## Enrollment Instructions

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

- 1. Welcome Page:** Enter the Activation Code provided above 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, after reviewing the Terms of Use, check the box to accept 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.

<sup>1</sup>Credit monitoring from Experian<sup>®</sup> and Transunion<sup>®</sup> will take several days to begin.

<sup>2</sup>The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

<sup>3</sup>Locking your Equifax credit file with Credit Report Control will prevent access to your Equifax credit file by certain third parties, such as credit grantors or other companies and agencies. Credit Report Control will not prevent access to your credit file at any other credit reporting agency, and will not prevent access to your Equifax credit file by companies like Equifax Global Consumer Solutions which provide you with access to your credit report or credit score or monitor your credit file; Federal, state and local government agencies; companies reviewing your application for employment; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; for fraud detection and prevention purposes; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit [www.optoutprescreen.com](http://www.optoutprescreen.com).

<sup>4</sup>Internet scanning will scan for your Social Security number (if you choose to), up to 5 bank accounts, up to 6 credit/debit card numbers that you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet Scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guaranteed that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

<sup>5</sup> Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.