

Appendix

On November 10, 2020, Indigo Contracting LLC identified a ransomware infection in its network. Upon learning this, Indigo retained Baker & Hostetler, LLP to provide legal advice and assistance investigating and responding to the incident. BakerHostetler then engaged cybersecurity consultants to conduct a forensic investigation to assist BakerHostetler in providing legal advice to Bosley.

On November 19, 2020, the forensic investigation identified unauthorized access to Indigo's email system. The email account was searched for any personal information. On January 20, 2021, Indigo identified the personal information of one Maine resident in the email account. The information included the individual's name and driver's license number.

On April 6, 2021, Indigo mailed a notification letter to the Maine resident pursuant to 10 M.R.S.A §§ 1346-1350-B.¹ A copy of the notification letter is attached. Indigo is offering the individual a one-year membership to credit monitoring and identity protection services.

To help prevent something like this from happening again, Indigo has updated passwords and implemented additional security safeguards and controls in its network infrastructure.

¹ This report does not waive Indigo's objection that Maine lacks personal jurisdiction over it related to any claims that may arise from this incident.



[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

April 11, 2021

Dear [REDACTED]

Indigo Contracting, LLC (“Indigo”) recognizes the importance of protecting information. We are writing to let you know of an incident that may have involved some of your information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.

We recently concluded an investigation into unauthorized access to one Indigo employee email account. Upon discovering the incident, we immediately took steps to secure the email account, a cybersecurity firm was engaged, and a thorough investigation was conducted. The investigation determined that there was unauthorized access to the email account on August 24, 2020.

The investigation was not able to determine whether any emails or attachments were actually viewed during that time. Therefore, we reviewed the contents of the email account to determine the specific individuals whose information it contained. We completed the review process on January 20, 2021. We then analyzed the results and determined that an email or attachment in the account contained some of your information, including your name, Social Security number and driver’s license number.

We wanted to notify you of this incident and assure you that we take it very seriously. As a precaution, we have arranged to provide you with a complimentary one-year membership in ID Patrol provided by Equifax. The service includes daily monitoring and alerts, dark web internet scanning, ID theft insurance and identity restoration. The service is completely free to you and enrolling in this program will not hurt your credit score. For more information, including instructions on how to activate your complimentary membership as well as some additional steps you can take to help protect yourself, please see the additional information provided with this letter.

We regret that this incident occurred and apologize for any inconvenience. To help prevent another incident from occurring, we are taking steps to further enhance our existing security measures. If you have any questions about the incident, please contact us at [telephone], from 8:30 am – 5:00 p.m. Mountain Time, Monday through Friday.

Sincerely,
Kevin Wright
President



Product Information

Enter your Activation Code: 

Equifax ID Patrol[®] provides you with the following key features:

- 3-Bureau credit file monitoring¹ and alerts of key changes to your Equifax[®], TransUnion[®] and Experian[®] 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 Alerts². With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit (available online only).
- Credit Report Lock³ Allows users to limit access to their Equifax credit report by third parties, with certain exceptions.
- Internet Scanning⁴ 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 insurance⁵
- 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

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.

¹Credit monitoring from Experian[®] and Transunion[®] will take several days to begin.

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

³Locking 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.

⁴Internet 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 guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

⁵ 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.

Experian[®] and TransUnion[®] are registered trademarks of their respective owners. Equifax[®] and ID Patrol[®] are registered trademarks. ©2017 Equifax Inc., Atlanta, Georgia. All rights reserved.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be 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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open

new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Washington: Indigo discovered the unauthorized access on November 19, 2020.