[**Full Name**]

[**Address Line 1**]

[**Address Line 2**]

[**City, State, Zip code**]

November 9, 2020

Notice of Data Breach

Dear [**Full Name**],

As previously noted in our email sent out on November 4, 2020, we are writing to provide you with an update regarding the recent disruption to Fresche Solutions Inc. ("**Fresche**")'s information technology systems.

Upon engaging a leading cybersecurity forensics firm to investigate this matter, Fresche learned that the service disruption was the result of a security incident involving an unauthorized third party, and that this incident may affect some of your personal information. We want you to be aware of the situation so you can take steps to protect yourself, including the steps we are taking to address this issue.

What Happened

On October 26, 2020, an unauthorized third party gained access to our servers, which resulted in the encryption of some of Fresche's information technology systems. On October 27, Fresche became aware of a system disruption on several critical servers, which alerted Fresche to the incident. Fresche took immediate action and has been working diligently to determine the scope of this incident, including engaging independent third-party cybersecurity experts to conduct a detailed investigation. This week, our investigation revealed that data may have been exfiltrated. The affected servers contained personal information of Fresche employees and contractors, as described in further detail below.

What Information Was Involved

The affected systems contained personal information of Fresche employees and contractors, and the following types of personal information could have been impacted by this incident:

- [Redacted]

What We Are Doing

The privacy and protection of your personal information is a matter we take very seriously, and we regret that this incident occurred. We are continuing to investigate the incident and are writing to inform you about what happened, what we are doing about it, and what steps you may wish to take to help protect yourself.

Our third-party cybersecurity experts took immediate steps to contain the incident, such as by disabling Fresche's virtual private network (VPN) connectivity and sanitizing and securing Fresche's information technology systems by resetting user accounts and deploying an Endpoint Detection & Response (EDR) technology, among other things. In addition, we have notified appropriate law enforcement authorities of this incident.

We are continuing to investigate and remediate this incident with the support of our cybersecurity experts and will provide follow-up communication, as we learn more.

What You Can Do

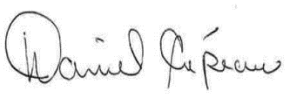
To help safeguard against any potential misuse of your personal information, we are offering credit monitoring and identity theft insurance through Equifax at no charge for the next 5 years. You may subscribe to this service by following the instructions enclosed.

Additionally, it is always a good idea to protect your personal information by monitoring your credit report, account statements, and online accounts. The “Additional Resources” insert, enclosed, provides more information regarding steps you can take to protect yourself, including your right to obtain a credit report, security freezes, or fraud alerts. You should exercise caution when responding to unsolicited communications that reference or request your personal information or account credentials.

For More Information

Again, we apologize for any inconvenience or alarm caused by this incident. Should you have any questions or concerns, please contact the Fresche HR department at HR@freschesolutions.com.

Regards,



Daniel Crepeau
President & CEO

Enter your Activation Code: [***INSERT ACTIVATION CODE***]
Enrollment Deadline: February 28th 2021

Product Information

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

- 3-Bureau credit file monitoring[1] 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 Alerts[2]. 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[3] Allows users to limit access to their Equifax credit report by third parties, with certain exceptions.
- Internet Scanning[4] 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[5].
- 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.

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

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

[3]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.

[4]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.

[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.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19022, 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** 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) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

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. More information regarding fraud alerts is available from credit reporting agencies or the FTC.

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 typically must be included when requesting a security freeze: (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 typically 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. More information regarding a security freeze is available from credit reporting agencies or the FTC.

Federal Trade Commission, State Attorneys General Offices, and law enforcement. 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 FTC, the Attorney General's office in your home state, or local law enforcement. You may also contact the FTC or your state Attorney General 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/, 1-877-IDTHEFT (438-4338).
- If you are a resident of North Carolina, you may contact the North Carolina Attorney General's Office, 114 West Edenton Street, Raleigh, NC 27603, www.ncdoj.gov/protecting-consumers/, 1-877-566-7226.