Christopherson

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

<<Full Name>>
<<Business Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

<<Date>>

Dear <<Full Name>>:

We write to make you aware of a recent data security incident at Christopherson Business Travel ("CBT") involving a limited amount of credit card information provided to us in connection with airfare we booked for you. CBT provides corporate airfare bookings for <<Data Owner or Entity>>. We wanted to provide you information about the incident and suggest steps you can take to protect yourself from credit card fraud.

What Happened?

On February 21, 2025, we detected unauthorized access to our network. We immediately engaged external forensic investigators and data privacy professionals and commenced a prompt and thorough investigation into the incident. As a result of this review, we determined on <<Variable Data 1>> that an unauthorized actor copied a limited amount of your information from our network on February 21, 2025.

What Information Was Involved?

The information that may have been acquired in this incident included your name, a payment card number, and payment card expiration date. We do not know whether the potentially compromised payment card information belongs to you or another party paying for your travel, as we routinely book business travel using a credit card supplied by a party other than the traveler. Additionally, no other personal information was compromised in this incident, including CVV codes, zip codes, or addresses. **We do not have any reports of fraudulent card activity as a result of this incident.**

What We Are Doing

We wanted to make you aware of the incident out of an abundance of caution. We also wanted to let you know what we are doing to further secure your information and suggest steps you can take to protect your information. Since learning of the incident, we have implemented enhanced security safeguards to help protect against similar intrusions.

What You Can Do

Below you will find precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant by reviewing your credit card statements for fraudulent or irregular activity on a regular basis. We are also providing you with 24 months of complimentary credit monitoring with Equifax. Please see below for enrollment instructions.

As a best practice, you should also call your bank or payment card issuer if you see any suspicious transactions. The policies of the payment card brands, such as Visa, MasterCard, American Express, and Discover, provide that you are not liable for

any unauthorized charges if you report them in a timely manner. You should also ask your bank or payment card issuer whether a new card should be issued to you if it has not been already.

For More Information

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line to respond to questions at 1-855-549-2608. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, **7:00** a.m. to **7:00** p.m. Mountain Time.

Thank you,

Christopherson Business Travel
Motor City Travel

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complementary Credit Monitoring

EQUIFAX®

<<Full Name>>
Enter your Activation Code: <<*ACTIVATION CODE*>>
Enrollment Deadline: <<Enrollment Deadline >>

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of <<*ACTIVATION CODE*>> then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. *[2]Credit monitoring from Experian and TransUnion will take several days to begin.* *[3]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of 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.* *[4]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.* *[5]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; 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.co* *[6]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

2. Placing a Fraud Alert.

You may place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

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

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-349-9960

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

To place the security freeze, 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 reporting company will send you a confirmation letter containing a unique personal identification number (PIN) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report with your local law enforcement agency.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the Federal Trade Commission (FTC) by contacting them on the internet at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-

438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Washington, D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 2001, https://oag.dc.gov/consumer-protection, Telephone: 1-202-727-3400.