

Hotel Vermont
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



<NAME>
<STREET>
<CITY>, <STATE> <ZIP>

A-75

April 6, 2021

NOTICE OF DATA SECURITY INCIDENT

Dear <NAME>:

Hotel Vermont, located in Burlington, Vermont (the “Hotel”), is writing to inform you of an incident that may affect the security of your personal information. The privacy and protection of our guests’ information is a matter we take extremely seriously. We are providing you with information and access to resources so that you can help protect against any potential misuse of your personal information, should you feel it appropriate to do so.

What Happened?

The Hotel utilizes a third party vendor, TravelClick, for online reservation services. On March 11, 2021, TravelClick informed us that the Hotel had been the victim of a phishing attack by a cybercriminal posing as a TravelClick representative. Using a deceptive e-mail and web portal, the cybercriminal captured, and then used, a Hotel employee’s TravelClick login credentials to access guest reservation records in Travel Click’s database. According to TravelClick, the cybercriminal was able to view guest reservation information within the Hotel’s TravelClick account database on January 21, 2021.

What Information Was Involved?

The records included payment card numbers, with and without expiration dates.

What Are We Doing?

The Hotel has taken steps to reduce the possibility of future similar incidents. All login credentials to its TravelClick accounts have been changed and, in cooperation with TravelClick, we implemented multifactor authentication for account logins. We are providing refresher training to employees in an effort to reinforce vigilance against social engineering threats of this type. We are also providing notice of this incident to appropriate state regulators, consistent with our compliance obligations and responsibilities. Additionally, we reported this incident to the Federal Bureau of Investigation (FBI).

What Can You Do?

We encourage you to remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges if they are reported in a timely fashion. If you believe your personal information is being misused, you should also notify your local law enforcement and state Attorney General. Additional information on ways to protect your information can be found at the end of this letter.

For More Information

We understand that you may have questions about this incident that are not addressed in this letter. You may use the contact information below for assistance with any questions you may have regarding this incident and steps you can take to protect your information.

We apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, please contact our designated hotline at 1-800-403-4529.

Sincerely,

A handwritten signature in black ink, appearing to read 'Hans van Wees', with a horizontal line underneath it.

Hans van Wees, General Manager
Hotel Vermont

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com	Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com
----------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------

You also may request a security freeze be added to your credit report at Experian's online Freeze Center, www.experian.com/freeze/center.html, by phone at 1-888-EXPERIAN (1-888-397-3742), or by mail to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013. More information on a security freeze can be found below.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

For Georgia, Maine 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.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically, which can help spot and address problems quickly.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. 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; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing 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. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

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, file a police report with your local law enforcement agency and contact your Attorney General. 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 FTC at the information provided above.

If this notice letter states that your financial account number and/or credit or debit card number was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

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 in the city in which you currently reside.

STATE SPECIFIC INFORMATION

DISTRICT OF COLUMBIA residents: You may also obtain information about preventing and avoiding identity theft from the D.C. Attorney General's Office. This office can be reached at:

Office of the Attorney General of the District of Columbia
Office of Consumer Protection
441 4th Street, NW
Washington, D.C. 20001
www.oag.dc.gov
1-202-727-3400

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State
Division of Consumer Protection
1-800-697-1220
<http://www.dos.ny.gov/consumerprotection>

New York Attorney General
1-800-771-7755
<http://www.ag.ny.gov/home.html>

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
Toll-free: 1-877-566-7226