Cooley

Via Certified Mail

Kris Kleiner
+1 720 566 4048
kkleiner@cooley.com

February 14, 2020

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sir or Madam:

I write on behalf of our client, Tablet Inc., to inform you of an information security incident involving limited personal data, specifically names, credit card details and billing addresses. The investigation determined that this incident affected the personal information of approximately five New Hampshire residents.

Tablet is an online travel agency that allows individuals to book stays at independent boutique and other similar hotels. This incident involved unauthorized access to the portal Tablet provides to hotels for hotels to access reservation data and add it to the hotel's property management system. The reservation and associated payment card information is available through the portal only for a brief period – long enough for the hotels to retrieve it – after which the information is no longer accessible through the portal. Based on the investigation, Tablet determined that an unauthorized third party accessed the online portal using compromised portal credentials and a software fault. In response, Tablet resolved the software fault and took steps to review and update its security measures, including by implementing two-factor authentication.

When Tablet detected the incident, it notified the hotels whose guests' information were accessed in the portal and coordinated with the hotels to provide notice to individuals and to appropriate regulators. Please note that some hotels may choose to notify individuals and/or regulators directly. Tablet has contacted law enforcement and will cooperate in any further investigation of this incident.

Individuals are being notified via email, which we expect will begin mailing on or around February 14, 2020. A form copy of the notice being sent to New Hampshire residents is included for your reference. If you have any questions or need further information regarding this incident, please contact me at (720) 566-4058 or kkleiner@cooley.com.

Sincerely,

Kristopher Kleiner

Enclosure

TABLET LETTERHEAD

[NAME]
[ADDRESS]

Dear [NAME]

This letter is to notify you of a security incident involving information related to a reservation you made for a hotel you booked on Tablet. This incident resulted in unauthorized access to the name, payment card details and billing address that you used to make the reservation. We sincerely regret that this incident occurred and any inconvenience it may have caused you.

This letter explains what is being done to address this incident, including our offer to provide you with identity protection and credit monitoring services for one year at no cost to you. When we detected the incident, we notified the hotels associated with the reservations involved, and we coordinated with the hotels to provide this notice.

What happened

An unauthorized third party accessed an online portal through which we made payment card information available to hotels so that the hotels could add that information to their property management systems. The payment card information is available through the portal only for a brief period – long enough for the hotel to retrieve it – after which the information is no longer accessible through the portal. An internal investigation that followed the discovery of the incident identified and addressed the incident's cause.

What information was involved

The reservation information involved was your name, billing address, payment card number, expiration date, and verification code. Specifically, this relates to reservation number [NUMBER] you made using a card ending in [LAST 4 DIGITS]. Please note that your email address and Tablet password were not affected by this incident.

What we are doing

We took steps to review and update our security measures as a result of this incident, as part of our continuous evaluation of the information security measures we have in place. This ongoing effort is part of our commitment to take the privacy and security of personal information seriously. Finally, law enforcement has been notified of the incident.

What you can do

Out of an abundance of caution, we have arranged for you to receive identity protection and credit monitoring services for one year at no cost to you. For more information about these services and instructions on completing the enrollment process, please refer to the enrollment instructions included in the attached Reference Guide. The Reference Guide also provides guidance on protecting your personal information and identity, including recommendations from the U.S. Federal Trade Commission.

For More Information

Please do not hesitate to contact us if you have additional questions. You can reach our dedicated support team via email at support@tablethotels.com or phone +1 (646) 880-6658, Mon-Fri, 9am - 5pm EST.

Sincerely,

Tablet Privacy Team

Reference Guide

To help protect your identity, we are offering a complimentary membership in Experian's® IdentityWorks®. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. Included with this service are fraud resolution services that provide an Experian Fraud Resolution agent to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). While this Fraud Resolution assistance is immediately available to you without any further action on your part, you can also activate the fraud detection tools available through enrolling in IdentityWorks® at no cost to you.

To enroll in these services, visit: **www.experianidworks.com/3bcredit** by **[DATE]**, and use the following activation code: **[ACTIVATION CODE]**. You may also enroll over the phone by calling **[PHONE]** between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **[ENGAGEMENT]**.

Once you enroll in IdentityWorks, you will have access to the following features:

- **Experian credit report at signup**: See what information is associated with your credit file.
- **Active Surveillance Alerts**: Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Fraud Resolution**: Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**[1]: Provides coverage for certain costs and unauthorized electronic fund transfers

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) -322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). 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.

information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC, and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.
- Report identity theft at www.IdentityTheft.gov.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-FTC-HELP (382-4357)
www.ftc.gov/idtheft
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. The initial fraud alert remains in place for a year. You can then continue to maintain a fraud alert on your credit file indefinitely by placing a new fraud alert each year. If you experience identity theft, you may request for your initial fraud alert to remain on your credit file for 7 years. You can place a fraud alert on your credit file by calling any one of the toll-free numbers provided below. You only need to call one of the credit reporting agencies – Equifax, Experian or TransUnion. The agency that you notify will alert the other two agencies to also place a fraud alert on your credit file. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-685-1111	www.Equifax.com/personal/credit-report-services
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/help
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-888-909-8872	www.transunion.com/credit-help

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to protect you from identity theft by requiring your express authorization before potential creditors may access your credit file at the consumer reporting agencies. Because a security freeze adds verification steps to the credit reporting process, the freeze may delay, interfere with, or prevent the approval of a loan or other credit you seek to obtain. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

Review Your Financial Accounts. Review your financial account statements to check for any discrepancies or unusual activity. If you see any account activity that you do not understand, contact the financial institution on whose account you found the activity immediately.

Change Account Passwords and Enable Multi-factor Authentication. Change the password to any account that could be affected by an incident. If you use the same or similar passwords for other online accounts, change your password for those accounts as well. You should use unique, "strong" passwords for all online accounts. You can find tips on creating strong passwords www.connectsafely.org/tips-to-create-and-manage-strong-passwords/. For accounts that support it, enable multi-factor authentication, which requires more than a username and password to access your account (e.g., a code texted to your phone, your fingerprint, or a number generated by a token or app).

For residents of Maryland. You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place

Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us.

For residents of Massachusetts. Massachusetts law gives you the right to place a security freeze on your consumer reports. By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request that a freeze be placed on your credit report, at no charge, by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and an incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

For residents of New Mexico. The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. For more information, including information about your rights under the FCRA, you can visit:

https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf
https://www.consumerfinance.gov/learnmore/

or write to:

Consumer Financial Protection Bureau
1700 G Street N.W.
Washington, DC 20552.

For residents of New York. You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/internet/privacy-and-identity-theft.

For residents of North Carolina. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov.

For residents of Rhode Island. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General, Consumer Protection Unit
150 South Main Street
Providence, RI 02903
401-274-4400
http://www.riag.ri.gov.