1900 M Street, NW, Suite 250 • Washington, D.C. 20036
202-706-5216 jason@zwillgen.com

ZwillGen PLLC

May 30, 2019

Attorney General Gordon MacDonald
New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General MacDonald:

On behalf of our client, Apple Inc. ("Apple"), we write to provide you with this notification of an incident that may have affected the personal information of one (1) New Hampshire resident. Apple recently learned that an associate employed by one of its service providers may have obtained a customer's payment card information without authorization and used it to make unauthorized purchases.

Apple's Risk and Compliance Team has determined that on February 2, 2019, an associate employed by Teleperformance AHA, a service provider to Apple, violated applicable call handling protocol by failing to turn off a screensharing tool while assisting a customer, which allowed her to see the customer's payment card information. When Apple discovered possible malfeasance by this Teleperformance associate via another customer's complaint, it initiated an investigation to review all of the associate's screen sharing sessions for evidence of additional breaches of protocol, which led to the discovery of this instance of possible wrongdoing. Teleperformance has suspended the employee while it investigates this matter further, and she has been removed from all Apple projects. While we have not yet been able to confirm whether the sales associate did, in fact, obtain any sensitive information without authorization, we are notifying affected customers of this incident out of an abundance of caution. The data elements potentially obtained by the third-party sales associate may have included the customer's name, billing/shipping address, email address, payment card account number, payment card expiration date, and payment card verification number (i.e., CVV2).

Apple has taken steps in response to this incident to help ensure that Teleperformance's employees follow established fraud prevention protocols. Apple is also offering the individual affected by this incident one year of complementary credit monitoring and identity theft protection services. A copy of the letter Apple is sending to the impacted customer is attached for your reference.

Should you have further questions about this matter, please do not hesitate to contact me at 202-706-5216 or jason@zwillgen.com.

Sincerely,

Jason R. Wool

May 30, 2019

[redacted]

NOTICE OF DATA BREACH

Dear [redacted]:

We are writing to notify you of an incident that may have affected the confidentiality of your personal information. Please read this letter carefully for more information and to learn how you can take steps to protect your personal information, including by enrolling in a complimentary year of Kroll Consumer Identity Monitoring and Consultation & Restoration Services.

What Happened?

On February 2, 2019, you participated in a screen sharing session with a sales associate who works for an Apple service provider, Teleperformance AHA. In light of an incident involving another customer and an investigation we initiated in response to that incident, we have reason to believe that the sales associate you spoke with may have copied some of your personal information without authorization. While we have not been able to confirm whether the third-party sales associate did, in fact, obtain your information, Apple has determined that she did not follow normal operating procedure for transactions like yours and could have done so. As a result, we are notifying you of this incident out of an abundance of caution.

What Information Was Involved?

The data elements potentially obtained by the sales associate may have included your name, billing/shipping address, email address, payment card account number, payment card expiration date, and payment card verification number (i.e., the number printed on the back of your payment card used in online and phone transactions to verify that you possess the card).

What We Are Doing.

In response to this incident, we have taken steps to help ensure that Teleperformance's employees follow established fraud prevention protocols. The Teleperformance employee has also been suspended while Apple and Teleperformance investigate this matter further, and she has been removed from all Apple projects. Finally, out of an abundance of caution we are providing you with one year of complimentary access to Kroll's Consumer Identity Monitoring and Consultation & Restoration Services. This product includes Kroll's Web Watcher, Public Persona, Quick Cash Scan, Online Triple Bureau Credit Monitoring, Fraud Consultation, Identity Theft Restoration, and $1M Identity Fraud Loss Reimbursement services. Additional Information on Kroll's services and instructions on how to enroll are provided below.

Apple
1 Infinite Loop
Cupertino, CA 95014

T 408 996-1010
F 408 996-0275
www.apple.com

What You Can Do.

In addition to enrolling in the Kroll credit monitoring service, we recommend that you 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 that are timely reported. There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please see the attachment to this letter.

For More Information.

If you have any questions regarding this incident or if you desire further information or assistance, please contact AppleCare at 408-862-0665. We regret any inconvenience caused by this incident. Please be assured that Apple takes the privacy and security of its customers' data very seriously and is taking steps to better ensure that incidents such as this one do not recur.

Sincerely,

Apple

SUPPLEMENTAL INFORMATION

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	Experian	TransUnion
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-685-1111	1-888-397-3742	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

If you are a resident of California or Maryland, you may contact and obtain information from and/or report identity theft to your state attorney general at:

California Attorney General's Office, California Department of Justice, Attn: Office of Privacy Protection, P.O. Box 944255, Sacramento, CA 94244-2550, (800) 952-5225

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or 1-410-576-6300

You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of 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 at least 90 days. 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

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

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Kroll

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services[1] include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by January 4, 2020. Your Activation Code will not work after this date.
2. Visit **redeem.kroll.com** to activate your identity monitoring services.
3. Provide Your Activation Code: [redacted] and Your Verification ID: [redacted]

1. To sign in to your account after you have activated your identity monitoring services, please visit **krollbreach.idmonitoringservice.com**

If you have questions, please call 1-866-775-4209, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

Take Advantage Of Your Identity Monitoring Services

You've been provided with access to the following services[1] from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report
Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher
Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona
Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan
Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement
Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.