



1900 M Street NW, Suite 250
Washington, DC 20036

Phone: (202) 296-3585
Website: www.zwillgen.com

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us
By email

July 20, 2022

Dear Attorney General Frosh:

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 three (3) Maryland residents. Apple recently learned that a customer service representative employed by one of Apple's service providers may have used customers' payment card information to make unauthorized purchases.

On June 30, 2022, Apple's Risk and Compliance Team identified that a number of customers had made similar complaints about unauthorized charges from non-Apple retailers appearing on their payment cards shortly after receiving assistance from the same Apple customer service representative. The representative in question was an employee of Concentrix, an Apple service provider. Upon learning of this incident, Apple undertook an investigation with Concentrix to determine whether unauthorized activity occurred. While a forensic investigation did not return any evidence that the representative acquired personal information without authorization, we are notifying customers and the Office of the Attorney General out of an abundance of caution.

The data elements that may have been misused by the customer service representative include customer's name, billing/shipping address, telephone number, email address, payment card account number, payment card expiration date, and payment card verification number (i.e., CVV2).

Following Apple's investigation, Concentrix terminated the customer service representative in question from Apple's account. Additionally, Apple is also notifying the individuals affected by this incident by mail and offering them one year of complementary credit monitoring and identity theft protection services. A copy of the letter Apple is sending to customers is attached for your reference.

Should you have further questions about this matter, please do not hesitate to contact me at 202-706-5226 or marci@zwillgen.com.

Sincerely,

Marci Rozen
Senior Legal Director, ZwillGen PLLC



[Date]

[Customer Name]

[Address]

Dear [Customer Name]:

We are writing to follow up with you about your recent inquiry regarding unauthorized purchases made on a payment card you used for a transaction with an Apple Care representative. 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 [Date], you notified us that an unauthorized purchase had been made on your payment card shortly after you used that card to complete a transaction facilitated by an Apple Care representative. Apple subsequently discovered that a Service Specialist (who is employed by an Apple vendor) may have inappropriately accessed your payment card information after your service call on [Date]. While Apple cannot definitively conclude whether the Service Specialist used your card to make purchases with third parties, we are notifying you of our findings so that you can take steps to secure your information.

What Information Was Involved?

The Service Specialist may have acquired information you provided during your interaction, such as your 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.

Upon receiving your inquiry, Apple promptly initiated an investigation together with our vendor to further understand what had occurred and to determine what the impact on your personal information may have been.

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
One Apple Park Way
Cupertino, CA 95014

T 408 996-1010
F 408 996-0275



What You Can Do.

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. For 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 letter or if you desire further information or assistance, please contact AppleCare at 669-283-4912. We regret any inconvenience caused by this issue.

Sincerely,

Apple Inc.



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
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-685-1111

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

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com
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, Connecticut, Iowa, Maryland, Massachusetts, North Carolina, Oregon, or Rhode Island, 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

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov

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



Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.nc-doj.gov, 1-919-716-6400 or 1-877-566-7226

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (503) 378-4400, <http://www.doj.state.or.us/>

Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

For other states: Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.

If you are a resident of Massachusetts or Rhode Island, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

If you are a resident of West Virginia, 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.

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.



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 services¹ 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 **XXX, 2023**. Your Activation Code will not work after this date.
2. Visit **Enroll.krollmonitoring.com/redeem** to activate your identity monitoring services.
3. Provide Your Activation Code: **<<Enter Activation Code>>** and Your Verification ID: **<<Enter Verification ID>>**

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services¹ 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 Chrome, Firefox, Safari and Edge. 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.