ZwillGen

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

November 4, 2024

To Whom It May Concern:

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) Maryland resident.

On October 30, 2024, Apple discovered that a third-party AppleCare vendor employee viewed the customer's payment card information in an unauthorized manner on October 17, 2024. While we do not have any direct evidence that unauthorized charges were placed on the card, we are notifying the Attorney General out of an abundance of caution.

The data elements that were accessed without authorization by the vendor employee include the customer's payment card account number, payment card expiration date, and payment card verification number, name, and billing address.

The vendor employee responsible for this incident no longer provides services to Apple. Additionally, Apple also notified the individual affected by this incident by mail on November 4, 2024, and is offering them one year of complementary credit monitoring and identity theft protection services. A template copy of the letter Apple sent to the customer 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

November 4, 2024

[Name]
[Address]

NOTICE OF DATA BREACH

Dear [name],

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 Experian Identity Works[SM].

What Happened?

On October 30, 2024, Apple discovered that an AppleCare vendor employee viewed your payment card information in an unauthorized manner. Our investigation revealed that this unauthorized access took place on [date]. While we do not have evidence of unauthorized charges placed on your payment card, we are notifying you so you can take steps to protect your payment account.

What Information Was Involved?

The information accessed without authorization by the AppleCare vendor employee includes 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), name, and billing address.

What We Are Doing.

Apple and its third-party vendor are investigating this incident, and the Specialist responsible for this incident no longer performs services for Apple. To further protect your information, we are providing you with one year of complimentary access to Experian Identity Works[SM].

What You Can Do.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including,

Apple
One Apple Park Way
Cupertino, CA 95014

T 408 996-1010
F 408 996-0275

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).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by 02/28/2025 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: **[CODE]**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by 02/28/2025. Be prepared to provide engagement number B134301 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- Credit Monitoring: Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARETM: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

In addition to enrolling in the Experian credit monitoring service, we recommend that you check for potential fraudulent charges on your payment card account, and remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring 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 the 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 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.

Free Credit Report. 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 9554	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	1-800-888-4213

Federal Trade Commission and State Attorneys General Reporting. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should 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 in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission and certain state Attorneys General Offices are as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.consumer.ftc.gov/features/identity-theft, 1-877-IDTHEFT (438-4338).
California Residents: California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.
Connecticut Residents: Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, www.ct.goviag, 1-860-808-5318.
District of Columbia Residents: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, www.oag.dc.gov, 1-202-727-3400.
Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, 1-502-696-5300.
Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, 1-888-743-0023.
Massachusetts Residents: Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, www.mass.gov/ago/contact-us.htnil, 1-617-727-8400.
New York Residents: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, https://ag.ny.gov/, 1-800-771-7755. North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, 1-919-716-6400.
Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, 877-877-9392.
Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 401-274-4400.

Fraud Alerts: 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. 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 request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number 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. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a security freeze 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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Experian Security Freeze P.O. Box 9554	TransUnion Security Freeze	Equifax Security Freeze
Allen, TX 75013	P.O. Box 160	P.O. Box 105788
	Chester, PA 19016	Atlanta, GA 30348
www.experian.com	www.transunion.com	www.equifax.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

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.