

10585



T2 US, LLC
Unilever North America
800 Sylvan Avenue
Englewood Cliffs, NJ 07632

Dear Vendor:

We wanted to make you aware that a T2 US, LLC ("T2") service provider was recently the subject of a security event, which impacts you. We are writing to tell you what happened and provide you with some steps you can take to help protect yourself against possible misuse of your information.

What Information was Involved?

T2 uses PKF O'Connor Davies, LLP ("PKFOD"), a public accounting firm, to prepare IRS Form 1099 for our vendors. PKFOD utilizes a third-party cloud storage and data hosting provider, Netgain Technology, LLC ("Netgain") to store data for our vendors. T2 has been informed that Netgain was the subject of a security event and your personal information may have been compromised by the security event. This information may include your name, address, Social Security Number, or financial account information.

Currently, efforts are being undertaken to determine if any data involved in this security event has been made available unlawfully, and to date, there is no evidence of data misuse.

What We Are Doing

T2 has been working with PKFOD to understand the security event and evaluate the remediation measures implemented by the cloud storage provider.

Additionally, we are offering you complimentary credit monitoring services provided by CyberScout for a period of twenty-four months. The services include access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring*** services and provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud, as well as a \$1,000,000 insurance reimbursement policy. Information on enrollment is included below.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do

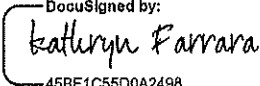
We encourage you to sign up for the complimentary services we are offering from CyberScout, using the instructions below. In addition, we encourage you to consider taking the following precautions:

- We urge you to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity. Report any unauthorized activity on your credit or banking accounts to your credit or banking providers immediately.
- If you suspect you are the victim of identity theft or fraud, you have the right to file a report with the police or law enforcement.
- You may contact the FTC or your state attorney general to learn more about the steps you can take to protect yourself against identity theft. The attachment to this letter titled "Information about Identity Theft Protection" has more information about steps you can take to protect yourself against identity theft or fraud.
- Be alert for "phishing" emails from someone who acts like they know you and requests sensitive information over email, such as passwords, Social Security numbers or bank account information.
- It is always best practice to change your financial account passwords often.

For More Information

For more information about this matter, or if you have additional questions or concerns, you may contact PKFOD at support@ODAdministration.com. We sincerely regret the concern or inconvenience that this matter may cause you.

Sincerely,

DocuSigned by:

45BF1C55D0A2498...
T2 US, LLC

Appendix A

How to Enroll in the Complimentary CyberScout Services

CyberScout representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 5:00 pm Eastern time, Monday through Friday. Please call the CyberScout help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

To enroll in Credit Monitoring* services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code: [REDACTED]. **Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. Please ensure you take this step to receive your alerts.** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Appendix B

Additional Information

To protect against possible fraud, identity theft, or other financial loss, you should always remain vigilant to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft, you can contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission (FTC). Please know that contacting us will not expedite any remediation of suspicious activity.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free from the U.S. at +1 (877) 726-1014.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You may contact any one of the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax: Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 +1 (888) 766-0008 www.equifax.com	Experian: Credit Fraud Center P.O. Box 9554 Allen, TX 75013 +1 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000 +1 (800) 680-7289 www.transunion.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 (5) years, the addresses where you have lived over those prior five (5) years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the FTC for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; by telephone at +1 (877) 382-4357; or at www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

California Residents: Visit the California Office of Privacy Protection (<https://oag.ca.gov/privacy>) for additional information on protection against identity theft.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.