From: The Omnipod Team <no_reply@theomnipodteam.com>
Sent: Thursday, January 5, 2023
To:
Subject: Notice of Data Privacy Incident

January 5, 2023

Dear Valued Customer,

We are contacting you because Insulet Corporation ("Insulet") recently experienced a data privacy incident that may affect some of your protected health information ("PHI"). Please review this notice carefully to learn about the incident and how it may affect a portion of your PHI.

What Happened?

Recently, Insulet sent a Medical Device Correction ("MDC") letter to Omnipod DASH® customers, including you. There was a follow-up receipt acknowledgment request sent by email. We believe that the configuration of web pages used for receipt verification exposed some limited personal information about you to certain Insulet website performance and marketing partners. No financial information, social security numbers, email addresses, or passwords were exposed. While no financial information was exposed in this incident, please see the **consumer notice (download PDF)** provided to you per state and federal law.

We sent out MDC acknowledgment request emails to certain customers, including you, on or about December 1, 2022. The e-mail included a clickable link to a unique verification page on the omnipod.com website. The URL (web page address) for each customer's unique page included: customer IP address (an internet protocol code number that may identify the location from which the webpage was accessed), whether customer is an Omnipod DASH user and whether customer has a Personal Diabetes Manager ("PDM"). These URLs were shared with website performance and marketing partners of Insulet through website "cookies" and/or other trackers embedded in the omnipod.com website code on the MDC acknowledgment web page.

We have completed an extensive review and investigation through which we identified you as a potentially affected individual.

What Information Was Involved?

Insulet believes that IP address, customer use of the Omnipod DASH product, and customer use of a PDM were exposed to website performance and marketing partners of Insulet.

What We are Doing

Insulet takes this event very seriously. After discovering the privacy incident on December 6, 2022, we disabled all tracking codes on the MDC acknowledgment web page that same day so that no further exposure of PHI as described in this letter could occur. Where possible, we are also requesting that our partners delete logs of the IP addresses and unique URLs so that they would not continue to have access to that information.

For More Information

If you have any further questions or concerns about this incident, feel free to contact us at our toll-free number 1-800-641-2049 or by email at privacy@insulet.com. We thank you for your continued support.

Sincerely,
David Harlow
Chief Compliance and Privacy Officer

Contact Us Privacy Policy FAQ

INS-ODS-01-2023-00002 v1.0

Insulet Corporation
100 Nagog Park, Acton, MA 01720

ADDITIONAL RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

The Federal Trade Commission

600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Credit Reporting Agencies

Equifax	**Experian**	**TransUnion**
PO Box 740241	PO Box 4500	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditregort.com. by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the

report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For Maryland Residents. 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 Massachusetts Residents: You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub or statement) in order to implement your request for a security freeze.There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center Raleigh,
NC 27699-9001
1-877-5-NO-SCAM
www.ncdoi.gov

For Rhode Island Residents: You have the right to obtain a police report. 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
1-401-274-4400
riag.ri.gov