Outset Medical
3052 Orchard Drive
San Jose, CA 95134
669.231.8200

Better
begins
now.

Dear Valued Consumer:

Outset Medical, Inc. ("Outset") is writing to inform you of a data security incident that affected certain of your personal information. At this time, we have no indication of fraud or misuse of your personal health information as a result of the incident. Nevertheless, we take the protection of your information seriously and are contacting you directly to explain the circumstances as we understand them, and the steps we have taken in response to the incident.

What Happened?

On September 14, 2023, Outset discovered that one of its employees had recently fallen victim to a phishing attack, and immediately took steps to re-secure the email account and investigate the scope and impact of the incident. While we have no indication of fraud or misuse as a result of this incident, your personal health information was available in the impacted account.

What Information May Have Been Involved?

Names, addresses, email addresses, and certain limited medical information were available in the impacted account. The medical information generally related to your or your care partner's web-based inquiries or other feedback about our home dialysis services. Importantly, your social security number, driver's license number, other government-issued ID, credit or debit card information or other financial information **were not impacted**.

What We Are Doing

We have secured the Outset employee's credentials and the impacted account and provided additional training and education to all employees regarding the risk of phishing attacks.

What You Can Do

We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information. As noted above, your social security number, driver's license number, other government-issued ID, credit or debit card information or other financial information **were not impacted**. Nevertheless, we provide enclosed additional tips you can consider taking to protect yourself against fraud and identity theft.

For More Information

The safety of our customers' personal information is of utmost importance to us. We take the security of customer information very seriously and sincerely regret any inconvenience. Should you have questions, please do not hesitate to contact us at privacy@outsetmedical.com. You may also contact Outset at 1-844-MY TABLO (1-844-698-2254).

Additional Ways to Protect Your Identity

Reviewing Your Accounts and Credit Reports

Federal regulators recommend that you to be vigilant in monitoring your financial accounts, regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289
Equifax.com	Experian.com	Transunion.com

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report. If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. Once one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge. If you wish to place a security freeze on your credit report, you must do so separately with each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing, or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you with a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan, a guide from the FTC to help you guard against and deal with identity theft. It is available online at* https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate

information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of Oregon and Rhode Island.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.