Notice of Data Breach

Dear Customer:

SwimOutlet.com is deeply invested in protecting the information of our customers. We are writing to inform you have we recently identified and addressed a security incident that may have involved your information. The intent of this letter is to explain the incident, the measures we have taken to address the incident, and some steps you may choose to take.

What Happened?
We identified a security incident on January 3rd, 2023 that involved the unauthorized disclosure of customer information on a publicly available code repository. We immediately implemented our security response plan, took steps to remove the repository, and launched an investigation into how the repository was created. A cyber security firm that has assisted other companies in similar situations was engaged. This notification was not delayed as a result of a law enforcement investigation.

What Information Was Involved?
The investigation identified that an employee created the repository accidentally and had not noticed it was public. We conducted a careful review of the files within the repository and, on January 4th, 2023, determined that the files contained information submitted to us via our Teams portal, including your name, phone number, and email address. No social security numbers, driver's license numbers, California identification card numbers or other unique identification numbers issued by government entities were included in the data files. We are not aware of any misuse of your information as a result of this Incident.

What We Are Doing.

We regret that this incident occurred and apologize for any inconvenience. To prevent something like this from happening again, we have taken steps to enhance our existing security measures. We have conducted an investigation to confirm the nature and scope of the activity and determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we further enhanced our technical and administrative policies and processes as part of our ongoing commitment to data security.

What You Can Do.
SwimOutlet is notifying you about this incident so you can protect yourself.

You can do this in several ways: by placing a fraud alert on your credit file; by placing a security freeze on your credit report; and by reviewing your credit reports regularly. We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity.

We also recommend that you review the identity theft materials posted for consumers on the Department of Homeland Security's website at: https://www.dhs.gov/employee-resources/blog/2021/01/21/preventing-identity-theft and on the Federal Trade Commission's (FTC) website at http://www.ftc.gov/idtheft. These websites provide detailed information about protecting yourself from identity theft and about steps to take if it occurs.

For More Information.
Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any questions, please call 1-800-469-7132, or contact shop@swimoutlet.com Monday through Friday, between 9:00 p.m. and 5 p.m. Pacific Standard Time

Sincerely,

Paul Knight
Director, IT and Security
SwimOutlet Security